Web UI Reference Guide

Product Model: xStack® DGS-3120 Series
Layer 2 Managed Stackable Gigabit Switch
Release 2.00

Information in this document is subject to change without notice.

© 2011 D-Link Corporation. All rights reserved.

Reproduction of this document in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

October 2011 P/N 651G312XX035G

Table of Contents

Intended Readers....1
Typographical Conventions....1
Notes, Notices and Cautions....1

Chapter 1 Web-based Switch Configuration....2

Introduction....2
Login to the Web Manager....2
Web-based User Interface....3
  Areas of the User Interface....3
Web Pages....4

Chapter 2 System Configuration....5

Device Information....5
System Information Settings....6
Port Configuration....6
  Port Settings....6
  Port Description Settings....8
  Port Error Disabled....9
  Jumbo Frame Settings....10
PoE....10
  PoE System Settings....11
  PoE Port Settings....12
Serial Port Settings....13
Warning Temperature Settings....13
System Log Configuration....14
  System Log Settings....14
  System Log Server Settings....14
  System Log....15
  System Log & Trap Settings....16
  System Severity Settings....17
Time Range Settings....18
Port Group Settings (EI Mode Only)....18
Time Settings....19
User Accounts Settings....19
Command Logging Settings....20
Configuration Trap Settings....21
Stacking....21
  Stacking Device Table....23
  Stacking Mode Settings....23

Chapter 3 Management....25

ARP....25
  Static ARP Settings....25
  Proxy ARP Settings (EI Mode Only)....26
  ARP Table....26
Gratuitous ARP....27
  Gratuitous ARP Global Settings....27
  Gratuitous ARP Settings....27
IPv6 Neighbor Settings (EI Mode Only)....28
IP Interface....29

System IP Address Settings 29
Interface Settings 30
Management Settings 33
Session Table 34
Single IP Management 34
Single IP Settings 36
Topology 37
Firmware Upgrade 43
Configuration File Backup/Restore 43
Upload Log File 44
SNMP Settings 44
SNMP Global Settings 45
SNMP Traps Settings 46
SNMP Linkchange Traps Settings 46
SNMP View Table Settings 47
SNMP Community Table Settings 48
SNMP Group Table Settings 49
SNMP Engine ID Settings 50
SNMP User Table Settings 50
SNMP Host Table Settings 51
SNMPv6 Host Table Settings (EI Mode Only) 52
RMON Settings 52
Telnet Settings 53
Web Settings 53
Power Saving 54
LED State Settings 54
Power Saving Settings 54
Power Saving LED Settings 55
Power Saving Port Settings 55
SD Card Management 56
SD Card Backup Settings 56
SD Card Execute Settings 56
Chapter 4 L2 Features 58
VLAN 58
802.1Q VLAN Settings 63
802.1v Protocol VLAN 66
Asymmetric VLAN Settings 68
GVRP 68
MAC-based VLAN Settings 70
Private VLAN Settings 70
PVID Auto Assign Settings 72
Voice VLAN 72
VLAN Trunk Settings 75
Browse VLAN 76
Show VLAN Ports 76
QinQ (EI Mode Only) 77
QinQ Settings 78
VLAN Translation Settings 79
Layer 2 Protocol Tunneling Settings 80
Spanning Tree 80

    STP Bridge Global Settings 82
    STP Port Settings 84
    MST Configuration Identification 85
    STP Instance Settings 86
    MSTP Port Information 86
  Link Aggregation 87
    Port Trunking Settings 89
    LACP Port Settings 90
  FDB 91
    Static FDB Settings 91
    MAC Notification Settings 92
    MAC Address Aging Time Settings 93
    MAC Address Table 94
    ARP & FDB Table 95
  L2 Multicast Control 95
    IGMP Snooping 95
    MLD Snooping 103
    Multicast VLAN 111
  Multicast Filtering 118
    IPv4 Multicast Filtering 118
    IPv6 Multicast Filtering 120
    Multicast Filtering Mode 122
  ERPS Settings (EI Mode Only) 123
  LLDP 126
    LLDP 127
    LLDP-MED 135
  NLB FDB Settings 138

Chapter 5 L3 Features 140
  IPv4 Default Route Settings (SI Mode Only) 140
  IPv4 Static/Default Route Settings (EI Mode Only) 140
  IPv4 Route Table 141
  IPv6 Static/Default Route Settings (EI Mode Only) 142
  IPv6 Route Table (EI Mode Only) 142
  IP Forwarding Table 143

Chapter 6 QoS 144
  802.1p Settings 145
    802.1p Default Priority Settings 145
    802.1p User Priority Settings 146
  Bandwidth Control 147
    Bandwidth Control Settings 147
    Queue Bandwidth Control Settings 148
  Traffic Control Settings 149
  DSCP 151
    DSCP Trust Settings 151
    DSCP Map Settings 152
  HOL Blocking Prevention 154
  Scheduling Settings 154
    QoS Scheduling 154
    QoS Scheduling Mechanism 155

Chapter 7 ACL 157

ACL Configuration Wizard....157
Access Profile List....158
  Add an Ethernet ACL Profile....159
  Adding an IPv4 ACL Profile....162
  Adding an IPv6 ACL Profile (EI Mode Only)....166
  Adding a Packet Content ACL Profile....170
CPU Access Profile List....174
  Adding a CPU Ethernet ACL Profile....175
  Adding a CPU IPv4 ACL Profile....178
  Adding a CPU IPv6 ACL Profile....182
  Adding a CPU Packet Content ACL Profile....185
ACL Finder....188
ACL Flow Meter....188
Egress Access Profile List (EI Mode Only)....191
  Add an Ethernet ACL Profile....192
  Adding an IPv4 ACL Profile....196
  Adding an IPv6 ACL Profile....199
Egress ACL Flow Meter (EI Mode Only)....203

Chapter 8 Security....206

802.1X....206
  802.1X Global Settings....209
  802.1X Port Settings....210
  802.1X User Settings....211
  Guest VLAN Settings....212
  Authenticator State....213
  Authenticator Statistics....214
  Authenticator Session Statistics....214
  Authenticator Diagnostics....215
  Initialize Port-based Port(s)....216
  Initialize Host-based Port(s)....217
  Reauthenticate Port-based Port(s)....217
  Reauthenticate Host-based Port(s)....218
RADIUS....218
  Authentication RADIUS Server Settings....218
  RADIUS Accounting Settings....219
  RADIUS Authentication....220
  RADIUS Account Client....221
IP-MAC-Port Binding (IMPB) (EI Mode Only)....223
  IMPB Global Settings....223
  IMPB Port Settings....223
  IMPB Entry Settings....225
  MAC Block List....225
  DHCP Snooping....226
MAC-based Access Control (MAC)....227
  MAC-based Access Control Settings....227
  MAC-based Access Control Local Settings....229
  MAC-based Access Control Authentication State....230
Web-based Access Control (WAC)....230
  WAC Global Settings....233
  WAC User Settings....234

- WAC Port Settings 235
- WAC Authentication State 236
- WAC Customize Page 236

Japanese Web-based Access Control (JWAC) 237

- JWAC Global Settings 237
- JWAC Port Settings 240
- JWAC User Settings 241
- JWAC Authentication State 241
- JWAC Customize Page Language 242
- JWAC Customize Page 242

Compound Authentication 244

- Compound Authentication Settings 244
- Compound Authentication Guest VLAN Settings (EI Mode Only) 246

IGMP Access Control Settings 246

Port Security 247

- Port Security Settings 247
- Port Security VLAN Settings 249
- Port Security Entries 250

ARP Spoofing Prevention Settings 250

BPDU Attack Protection 251

Loopback Detection Settings 252

RPC PortMapper Filter Settings 254

NetBIOS Filtering Settings 254

Traffic Segmentation Settings 255

DHCP Server Screening 256

- DHCP Server Screening Port Settings 256
- DHCP Offer Permit Entry Settings 257

Access Authentication Control 258

- Enable Admin 259
- Authentication Policy Settings 260
- Application Authentication Settings 261
- Authentication Server Group Settings 261
- Authentication Server Settings 263
- Login Method Lists Settings 264
- Enable Method Lists Settings 265
- Local Enable Password Settings 266

SSL Settings 266

SSH 268

- SSH Settings 269
- SSH Authentication Method and Algorithm Settings 270
- SSH User Authentication List 271

Trusted Host Settings 272

Safeguard Engine Settings 274

Chapter 9 Network Application 277

DHCP 277

- DHCP Relay 277
- DHCPv6 Relay (EI Mode Only) 283
- DHCP Local Relay Settings 284

PPPoE Circuit ID Insertion Settings (EI Mode Only) 284

SMTP Settings 285

- SNTP 286
  - SNTP Settings 286
  - Time Zone Settings 287
- Flash File System Settings 289

Chapter 10 OAM 291

- CFM (EI Mode Only) 291
  - CFM Settings 291
  - CFM Port Settings 297
  - CFM MIPCCM Table 297
  - CFM Loopback Settings 298
  - CFM Linktrace Settings 298
  - CFM Packet Counter 299
  - CFM Fault Table 300
  - CFM MP Table 301
- Ethernet OAM (EI Mode Only) 301
  - Ethernet OAM Settings 301
  - Ethernet OAM Configuration Settings 302
  - Ethernet OAM Event Log 303
  - Ethernet OAM Statistics 304
- DULD Settings (EI Mode Only) 305
- Cable Diagnostics 306

Chapter 11 Monitoring 308

- Utilization 308
  - CPU Utilization 308
  - DRAM & Flash Utilization 308
  - Port Utilization 309
- Statistics 310
  - Port Statistics 310
  - Packet Size 318
- Mirror 319
  - Port Mirror Settings 319
  - RSPAN Settings 320
- sFlow (EI Mode Only) 322
  - sFlow Global Settings 322
  - sFlow Analyzer Server Settings 322
  - sFlow Flow Sampler Settings 323
  - sFlow Counter Poller Settings 324
- Ping Test 324
- Trace Route 326
- Peripheral 327
  - Device Environment 327

Chapter 12 Save and Tools 328

- Save Configuration / Log 328
- Stacking Information 328
- Download firmware 330
  - Download Firmware From TFTP 330
  - Download Firmware From HTTP 330
- Upload Firmware 331
  - Upload Firmware To TFTP 331
- Download Configuration 332

Download Configuration From TFTP....332
Download Configuration From HTTP....333
Upload Configuration....333
Upload Configuration To TFTP....333
Upload Configuration To HTTP....334
Upload Log File....335
Upload Log To TFTP....335
Upload Log To HTTP....335
Reset....336
Reboot System....336
Appendix Section....338
Appendix A Mitigating ARP Spoofing Attacks Using Packet Content ACL....338
How Address Resolution Protocol works....338
How ARP Spoofing Attacks a Network....340
Prevent ARP Spoofing via Packet Content ACL....341
Configuration....341
Appendix B Password Recovery Procedure....344
Appendix C System Log Entries....345
Appendix D Trap Log Entries....355
Appendix E RADIUS Attributes Assignment....361

Intended Readers

Typographical Conventions
Notes, Notices and Cautions
Safety Instructions
General Precautions for Rack-Mountable Products
Protecting Against Electrostatic Discharge

The ***DGS-3120 Series Web UI Reference Guide*** contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
`[]`	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. **Bold** font is also used to represent filenames, program names and commands. For example: **use the copy command**.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices and Cautions

A **NOTE** indicates important information that helps make better use of the device.

A **NOTICE** indicates either potential damage to hardware or loss of data and tells how to avoid the problem.

A **CAUTION** indicates a potential for property damage, personal injury, or death.

Chapter 1 Web-based Switch Configuration

Introduction
Login to the Web Manager
Web-based User Interface
Web Pages

Introduction

All software functions of the DGS-3120 Series switches can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

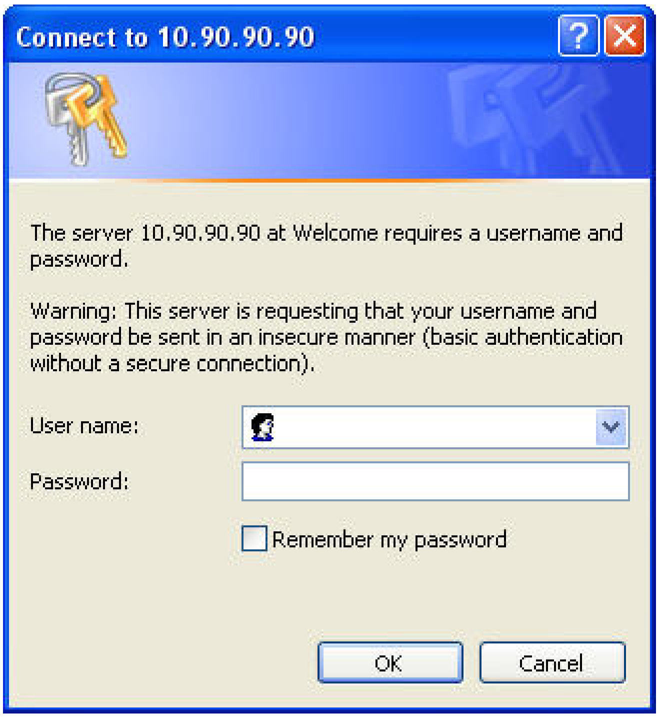
The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Login to the Web Manager

To begin managing the Switch, simply run the browser installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE: The factory default IP address is 10.90.90.90.

This opens the management module's user authentication window, as seen below.



Connect to 10.90.90.90

The server 10.90.90.90 at Welcome requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Figure 1-1 Enter Network Password window

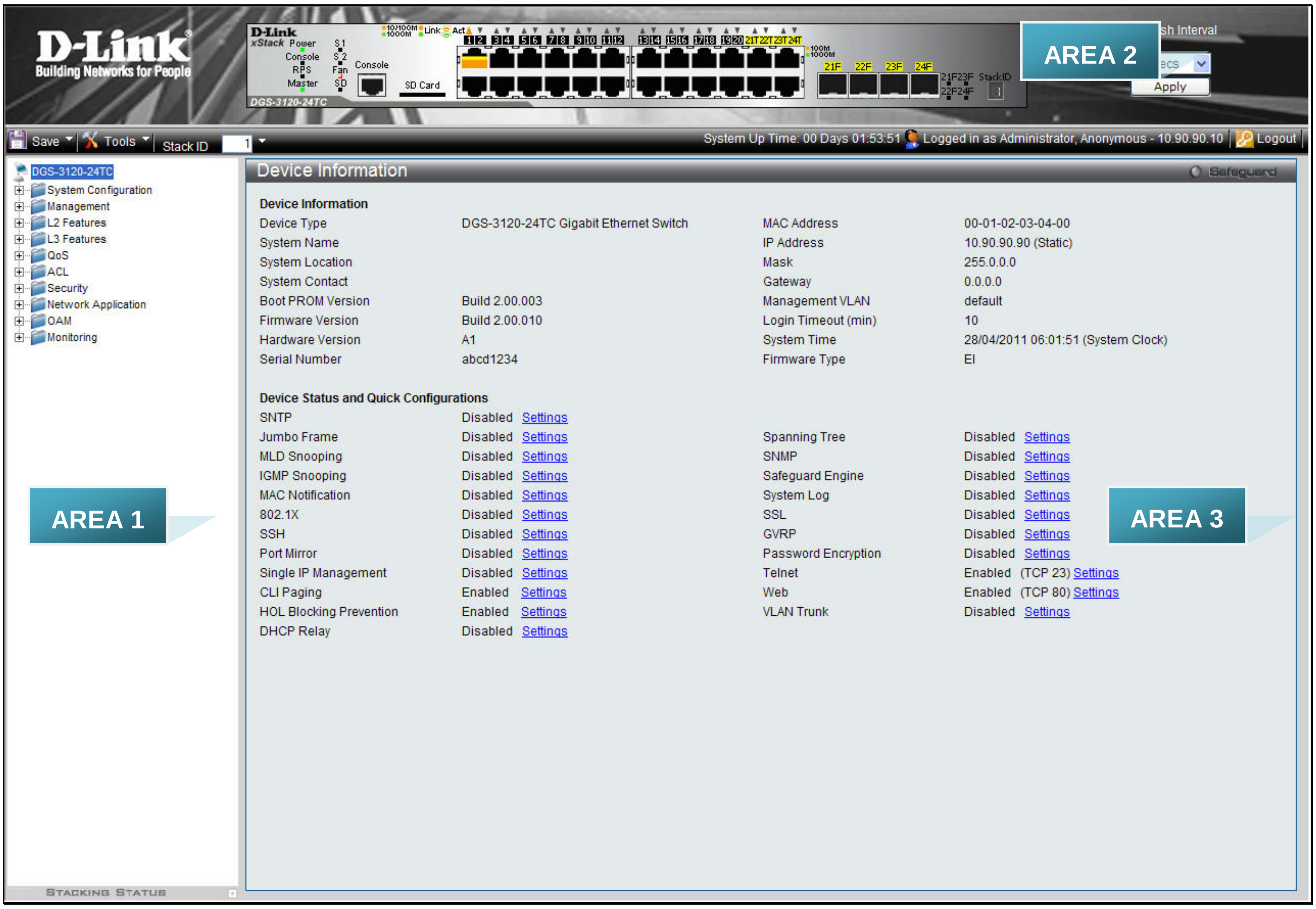
Leave both the **User Name** field and the **Password** field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas divide the user interface, as described in the table.


D-Link
Building Networks for People
D-Link xStack
Power
Console
RPS
Master
S1
S2
Fan
SD
Console
SD Card
DGS-3120-24TC
10/100M 1000M
Link
Act
21F
22F
23F
24F
StackID
AREA 2
sh Interval
ecs
Apply
Save
Tools
Stack ID
1
Logout
DGS-3120-24TC
System Configuration
Management
L2 Features
L3 Features
QoS
ACL
Security
Network Application
OAM
Monitoring
STACKING STATUS
Safeguard
AREA 1
AREA 3

System Up Time: 00 Days 01:53:51 Logged in as Administrator, Anonymous - 10.90.90.10

Device Information

Device Information

Device Type	DGS-3120-24TC Gigabit Ethernet Switch	MAC Address	00-01-02-03-04-00
System Name		IP Address	10.90.90.90 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	Build 2.00.003	Management VLAN	default
Firmware Version	Build 2.00.010	Login Timeout (min)	10
Hardware Version	A1	System Time	28/04/2011 06:01:51 (System Clock)
Serial Number	abcd1234	Firmware Type	EI

Device Status and Quick Configurations

SNTP	Disabled Settings		
Jumbo Frame	Disabled Settings	Spanning Tree	Disabled Settings
MLD Snooping	Disabled Settings	SNMP	Disabled Settings
IGMP Snooping	Disabled Settings	Safeguard Engine	Disabled Settings
MAC Notification	Disabled Settings	System Log	Disabled Settings
802.1X	Disabled Settings	SSL	Disabled Settings
SSH	Disabled Settings	GVRP	Disabled Settings
Port Mirror	Disabled Settings	Password Encryption	Disabled Settings
Single IP Management	Disabled Settings	Telnet	Enabled (TCP 23) Settings
CLI Paging	Enabled Settings	Web	Enabled (TCP 80) Settings
HOL Blocking Prevention	Enabled Settings	VLAN Trunk	Disabled Settings
DHCP Relay	Disabled Settings		

Figure 1-2 Main Web-Manager page

Area Number	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports, console and management port, showing port activity. Some management functions, including save, reboot, download and upload are accessible here.
Area 3	Presents switch information based on user selection and the entry of configuration data.

Web Pages

When connecting to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list of the main folders available in the Web interface:

System Configuration - In this section the user will be able to configure features regarding the Switch's configuration.

Management - In this section the user will be able to configure features regarding the Switch's management.

L2 Features - In this section the user will be able to configure features regarding the Layer 2 functionality of the Switch.

L3 Features - In this section the user will be able to configure features regarding the Layer 3 functionality of the Switch.

QoS - In this section the user will be able to configure features regarding the Quality of Service functionality of the Switch.

ACL - In this section the user will be able to configure features regarding the Access Control List functionality of the Switch.

Security - In this section the user will be able to configure features regarding the Switch's security.

Network Application - In this section the user will be able to configure features regarding network applications handled by the Switch.

OAM - In this section the user will be able to configure features regarding the Switch's operations, administration and maintenance (OAM).

Monitoring - In this section the user will be able to monitor the Switch's configuration and statistics.

NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Chapter 2 System Configuration

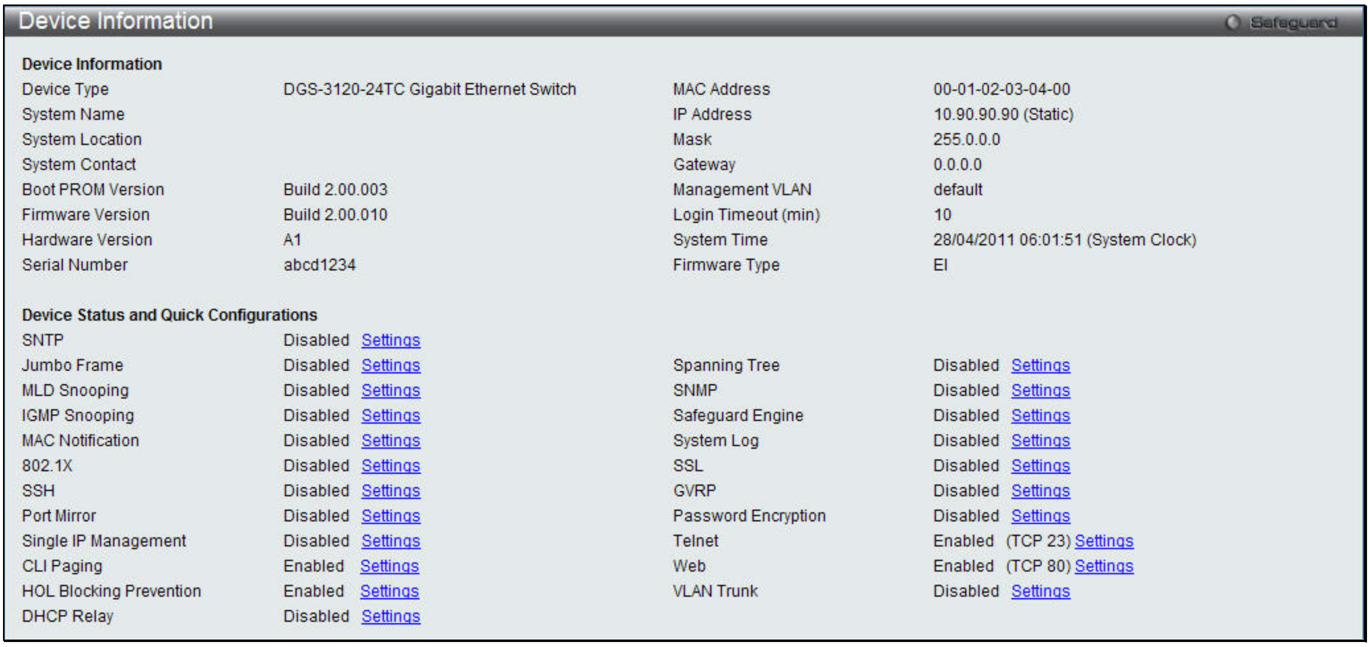
Device Information
System Information Settings
Port Configuration
PoE
Serial Port Settings
Warning Temperature Settings
System Log configuration
Time Range Settings
Port Group Settings (EI Mode Only)
Time Settings
User Accounts Settings
Command Logging Settings
Configuration Trap Settings
Stacking

Device Information

This window contains the main settings for all the major functions for the Switch. It appears automatically when you log on to the Switch. To return to the Device Information window after viewing other windows, click the **DGS-3120 Series** link.

The Device Information window shows the Switch's MAC Address (assigned by the factory and unchangeable), the Boot PROM Version, Firmware Version, Hardware Version, and many other important types of information. This is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. In addition, this window displays the status of functions on the Switch to quickly assess their current global status.

Many functions are hyper-linked for easy access to enable quick configuration from this window.



Device Information

Device Type	DGS-3120-24TC Gigabit Ethernet Switch	MAC Address	00-01-02-03-04-00
System Name		IP Address	10.90.90.90 (Static)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	Build 2.00.003	Management VLAN	default
Firmware Version	Build 2.00.010	Login Timeout (min)	10
Hardware Version	A1	System Time	28/04/2011 06:01:51 (System Clock)
Serial Number	abcd1234	Firmware Type	EI

Device Status and Quick Configurations

SNTP	Disabled Settings		
Jumbo Frame	Disabled Settings	Spanning Tree	Disabled Settings
MLD Snooping	Disabled Settings	SNMP	Disabled Settings
IGMP Snooping	Disabled Settings	Safeguard Engine	Disabled Settings
MAC Notification	Disabled Settings	System Log	Disabled Settings
802.1X	Disabled Settings	SSL	Disabled Settings
SSH	Disabled Settings	GVRP	Disabled Settings
Port Mirror	Disabled Settings	Password Encryption	Disabled Settings
Single IP Management	Disabled Settings	Telnet	Enabled (TCP 23) Settings
CLI Paging	Enabled Settings	Web	Enabled (TCP 80) Settings
HOL Blocking Prevention	Enabled Settings	VLAN Trunk	Disabled Settings
DHCP Relay	Disabled Settings		

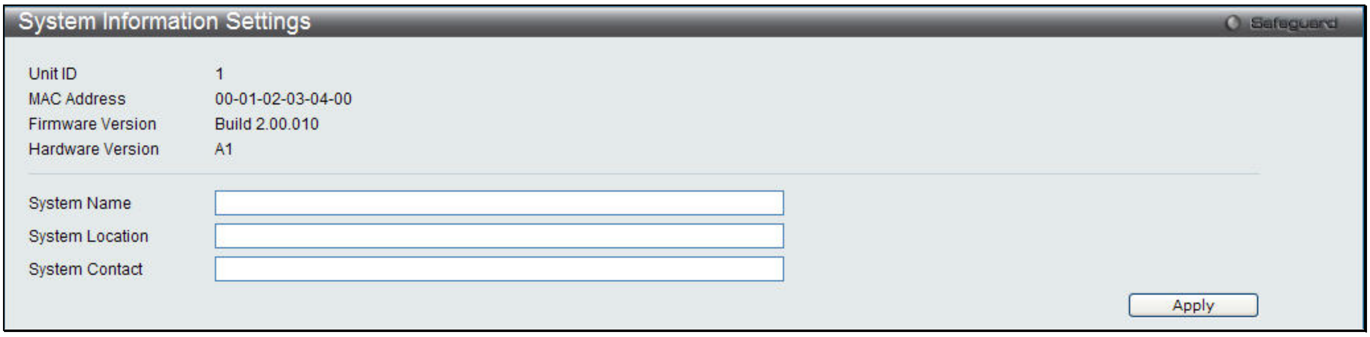
Figure 2-1 Device Information window

Click the Settings link to navigate to the appropriate feature page for configuration.

System Information Settings

The user can enter a **System Name, System Location**, **and System Contact** to aid in defining the Switch.

To view the following window, click **System Configuration > System Information Settings**, as show below:



Unit ID 1
MAC Address 00-01-02-03-04-00
Firmware Version Build 2.00.010
Hardware Version A1
System Name
System Location
System Contact

Figure 2-2 System Information Settings window

The fields that can be configured are described below:

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.

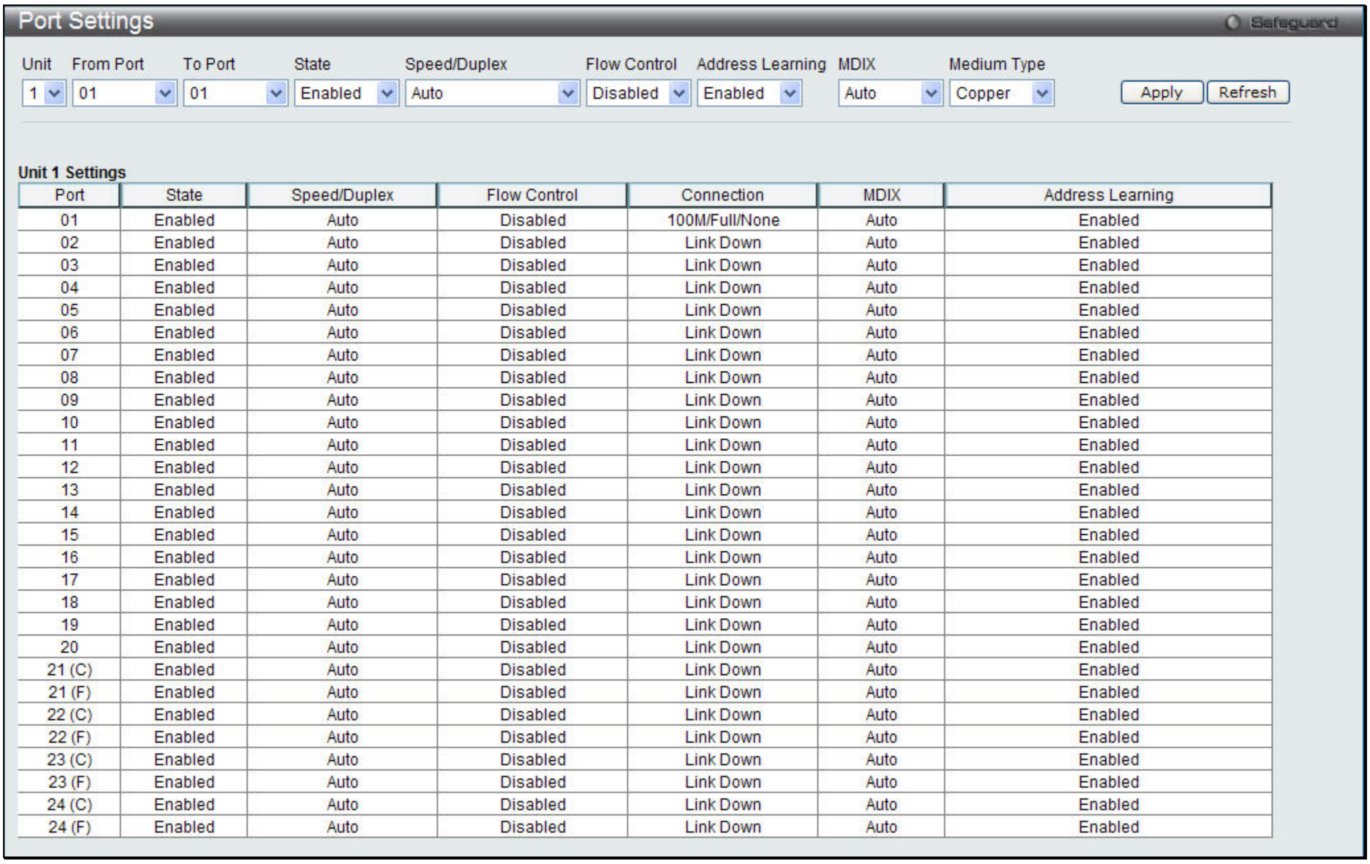
Click the **Apply** button to implement changes made.

Port Configuration

Port Settings

This page used to configure the details of the switch ports.

To view the following window, click **System Configuration > Port Configuration > Port Settings**, as show below:



Unit	From Port	To Port	State	Speed/Duplex	Flow Control	Address Learning	MDIX	Medium Type
1	01	01	Enabled	Auto	Disabled	Enabled	Auto	Copper

Unit 1 Settings

Port	State	Speed/Duplex	Flow Control	Connection	MDIX	Address Learning
01	Enabled	Auto	Disabled	100M/Full/None	Auto	Enabled
02	Enabled	Auto	Disabled	Link Down	Auto	Enabled
03	Enabled	Auto	Disabled	Link Down	Auto	Enabled
04	Enabled	Auto	Disabled	Link Down	Auto	Enabled
05	Enabled	Auto	Disabled	Link Down	Auto	Enabled
06	Enabled	Auto	Disabled	Link Down	Auto	Enabled
07	Enabled	Auto	Disabled	Link Down	Auto	Enabled
08	Enabled	Auto	Disabled	Link Down	Auto	Enabled
09	Enabled	Auto	Disabled	Link Down	Auto	Enabled
10	Enabled	Auto	Disabled	Link Down	Auto	Enabled
11	Enabled	Auto	Disabled	Link Down	Auto	Enabled
12	Enabled	Auto	Disabled	Link Down	Auto	Enabled
13	Enabled	Auto	Disabled	Link Down	Auto	Enabled
14	Enabled	Auto	Disabled	Link Down	Auto	Enabled
15	Enabled	Auto	Disabled	Link Down	Auto	Enabled
16	Enabled	Auto	Disabled	Link Down	Auto	Enabled
17	Enabled	Auto	Disabled	Link Down	Auto	Enabled
18	Enabled	Auto	Disabled	Link Down	Auto	Enabled
19	Enabled	Auto	Disabled	Link Down	Auto	Enabled
20	Enabled	Auto	Disabled	Link Down	Auto	Enabled
21 (C)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
21 (F)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
22 (C)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
22 (F)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
23 (C)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
23 (F)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
24 (C)	Enabled	Auto	Disabled	Link Down	Auto	Enabled
24 (F)	Enabled	Auto	Disabled	Link Down	Auto	Enabled

Figure 2-3 Port Settings window

To configure switch ports:

1. Choose the port or sequential range of ports using the From Port and To Port drop-down menus.
2. Use the remaining drop-down menus to configure the parameters described below:

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Toggle the State field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the Speed/Duplex field to select the speed and full-duplex/half-duplex state of the port. *Auto* denotes auto-negotiation among 10, 100 and 1000 Mbps devices, in full- or half-duplex (except 1000 Mbps which is always full duplex). The *Auto* setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are *10M Half*, *10M Full, 100M Half*, *100M Full*, *1000M Full_Master*, *1000M Full_Slave, and 1000M Full*. There is no automatic adjustment of port settings with any option other than *Auto*. The Switch allows the user to configure three types of gigabit connections; *1000M Full_Master*, *1000M Full_Slave*, and *1000M Full*. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed. The *1000M Full_Master* and *1000M Full_Slave* parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (*1000M Full_Master)* will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between

	the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (*1000M Full_Slave)* uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for *1000M Full_Master*, the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is *Disabled*.
Connection	Here the current connection speed will be displayed.
MDIX	*Auto* - Select auto for auto sensing of the optimal type of cabling. *Normal* - Select normal for normal cabling. If set to normal state, the port is in MDI mode and can be connected to a PC NIC using a straight-through cable or a port (in MDI mode) on another switch through a cross-over cable. *Cross* - Select cross for cross cabling. If set to cross state, the port is in MDIX mode, and can be connected to a port (in MDI mode) on another switch through a straight cable.
Address Learning	Enable or disable MAC address learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When address learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is *Enabled*.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used.

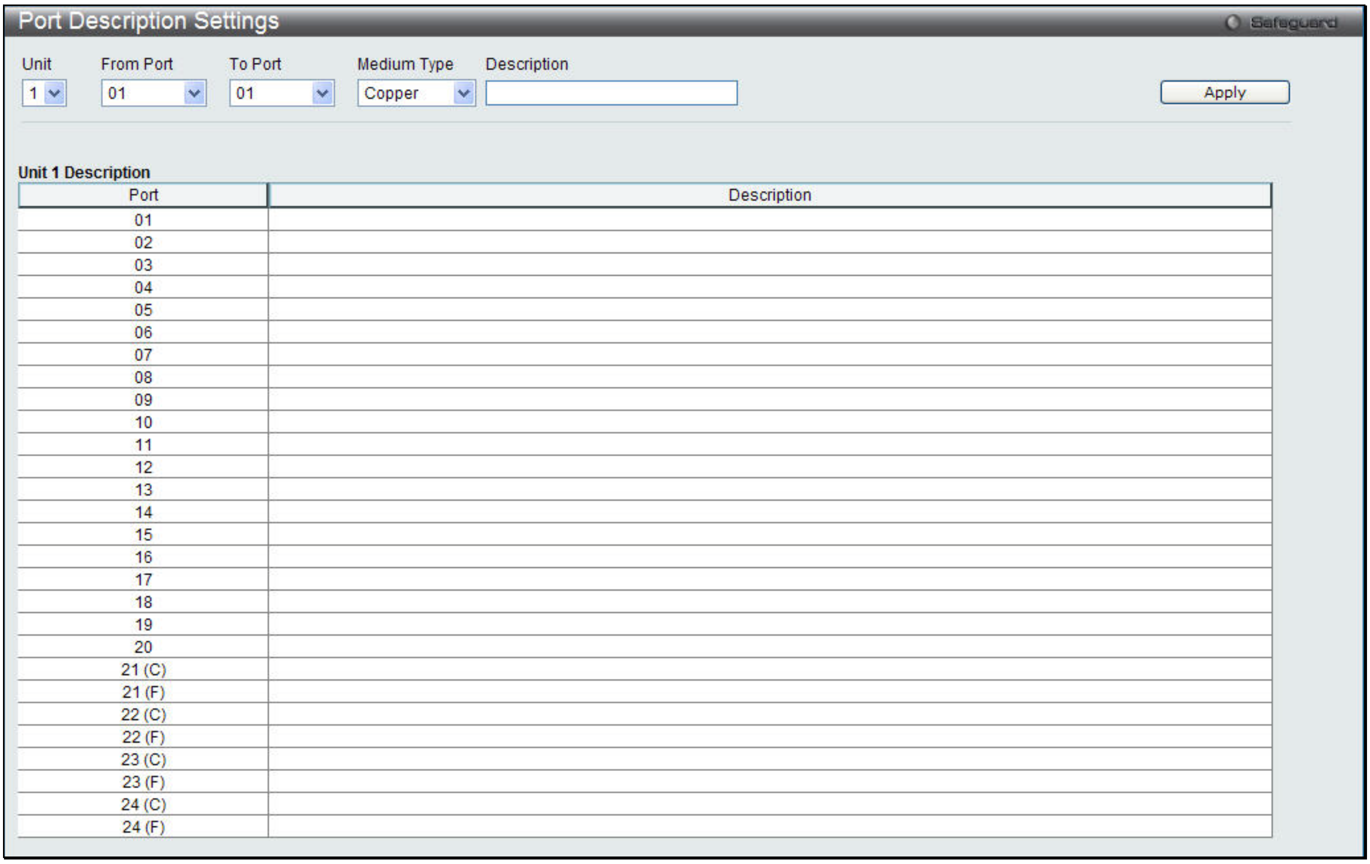
Click the **Apply** button to implement changes made.

Click the **Refresh** button to refresh the display section of this page.

Port Description Settings

The Switch supports a port description feature where the user may name various ports.

To view the following window, click **System Configuration > Port Configuration > Port Description Settings**, as show below:



Port Description Settings

Unit: 1
From Port: 01
To Port: 01
Medium Type: Copper
Description:

Unit 1 Description

Port	Description
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21 (C)	
21 (F)	
22 (C)	
22 (F)	
23 (C)	
23 (F)	
24 (C)	
24 (F)	

Figure 2-4 Port Description Settings window

The fields that can be configured are described below:

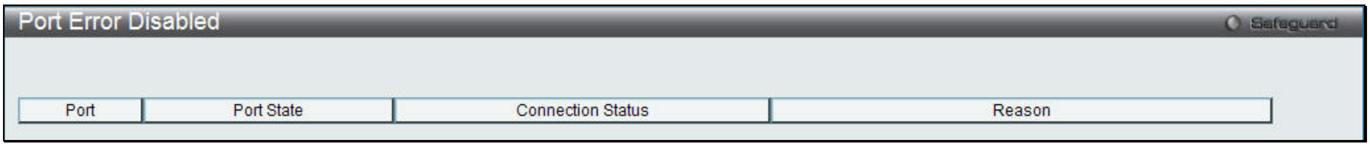
Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Select the appropriate port range used for the configuration here.
Medium Type	Specify the medium type for the selected ports. If configuring the Combo ports, the Medium Type defines the type of transport medium to be used, whether *Copper* or *Fiber.*
Description	Users may then enter a description for the chosen port(s).

Click the **Apply** button to implement changes made.

Port Error Disabled

The following window displays the information about ports that have been disconnected by the Switch when a packet storm occurs or a loop was detected.

To view the following window, click **System Configuration > Port Configuration > Port Error Disabled**, as show below:



Port Error Disabled

Port	Port State	Connection Status	Reason

Figure 2-5 Port Error Disabled

The fields that can be displayed are described below:

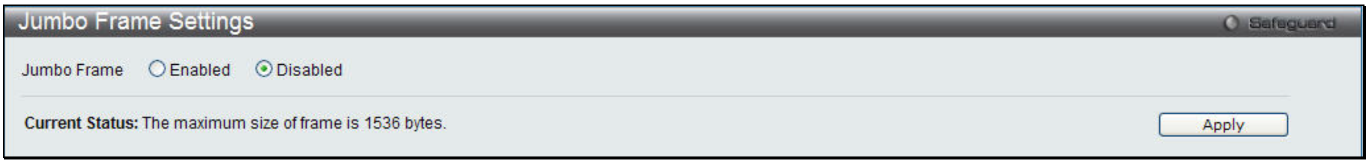
Parameter	Description
Port	Display the port that has been error disabled.

Port State	Describe the current running state of the port, whether enabled or disabled.
Connection Status	Display the uplink status of the individual ports, whether enabled or disabled.
Reason	Describe the reason why the port has been error-disabled, such as it has become a shutdown port for storm control.

Jumbo Frame Settings

The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 13312 bytes.

To view the following window, click **System Configuration > Port Configuration > Jumbo Frame Settings**, as show below:



Jumbo Frame ○ Enabled ● Disabled

Current Status: The maximum size of frame is 1536 bytes.

Figure 2-6 Jumbo Frame Settings window

The fields that can be configured are described below:

Parameter	Description
Jumbo Frame	Use the radio buttons to enable or disable the Jumbo Frame function on the Switch. The default is Disabled. When disabled, the maximum frame size is 1536 bytes. When enabled, the maximum frame size is 13312 bytes.

Click the **Apply** button to implement changes made.

PoE

The DGS-3120-24PC and DGS-3120-48PC switches support Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 3 UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The Switches work with all D-Link 802.3af capable devices.

The Switch includes the following PoE features:

- Auto-discovery recognizes the connection of a PD (Powered Device) and automatically sends power to it.
- The Auto-disable feature occurs under two conditions: firstly, if the total power consumption exceeds the system power limit; and secondly, if the per port power consumption exceeds the per port power limit.
- Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Based on 802.3af/at PDs receive power according to the following classification:

Class	Maximum power available to PD
0	15.4W
1	4.0W
2	7.0W
3	15.4W
4	15.4W

PSE provides power according to the following classification:

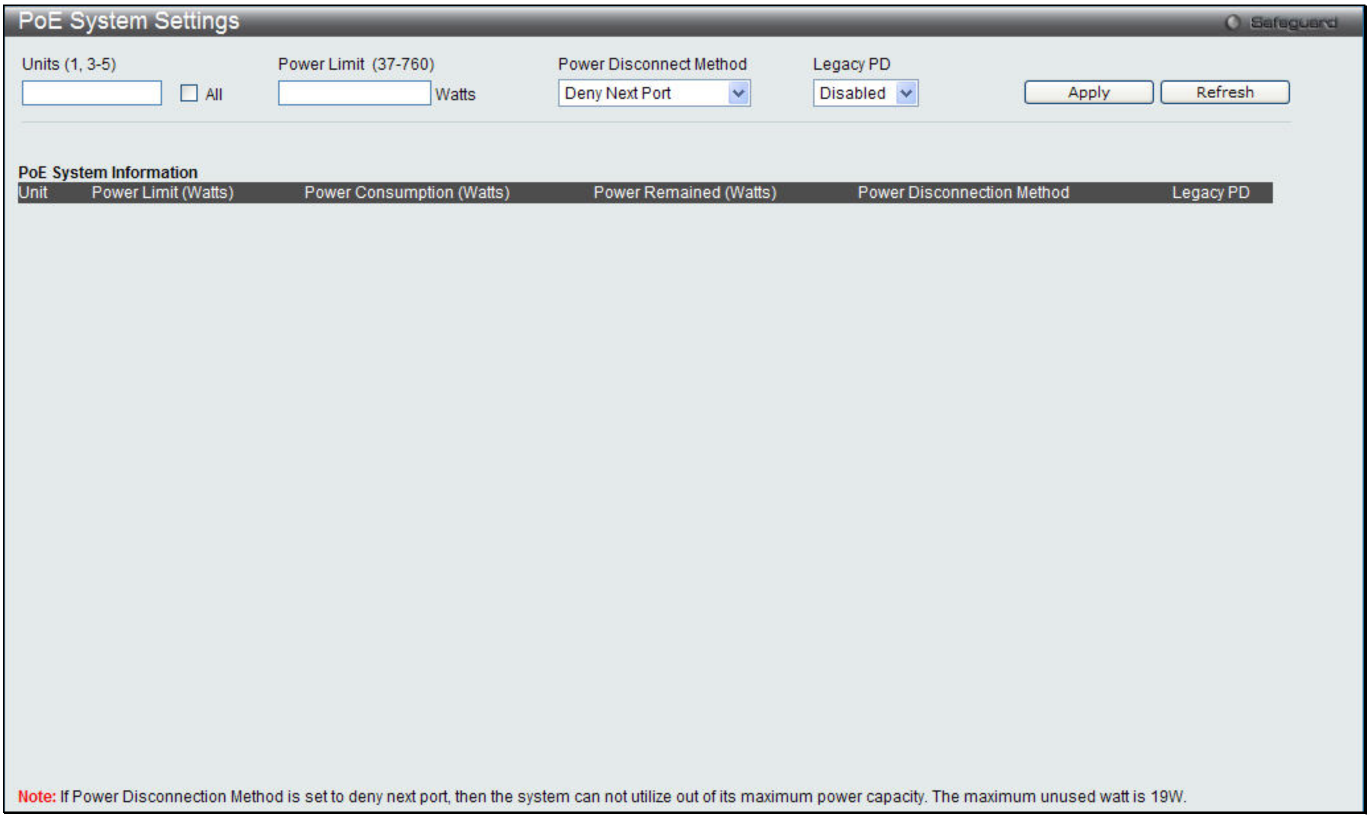
Class	Max power used by PSE
0	16.2W
1	4.2W
2	7.4W
3	16.2W
User define	31.2W

To configure the PoE features on the Switch, click **System Configuration > PoE**. The **PoE System Settings** window is used to assign a power limit and power disconnect method for the whole PoE system. To configure the **Power Limit** for the PoE system, enter a value between 1W and 370W for the Switch in the Power Limit field.

When the total consumed power exceeds the power limit, the PoE controller (located in the PSE) disconnects the power to prevent overloading the power supply.

PoE System Settings

To view the following window, click **System Configuration > PoE > PoE System Settings**, as show below:



Power Disconnect Method: Deny Next Port

Legacy PD: Disabled

PoE System Information

Unit	Power Limit (Watts)	Power Consumption (Watts)	Power Remained (Watts)	Power Disconnection Method	Legacy PD

Note: If Power Disconnection Method is set to deny next port, then the system can not utilize out of its maximum power capacity. The maximum unused watt is 19W.

Figure 2-7 PoE System Settings window

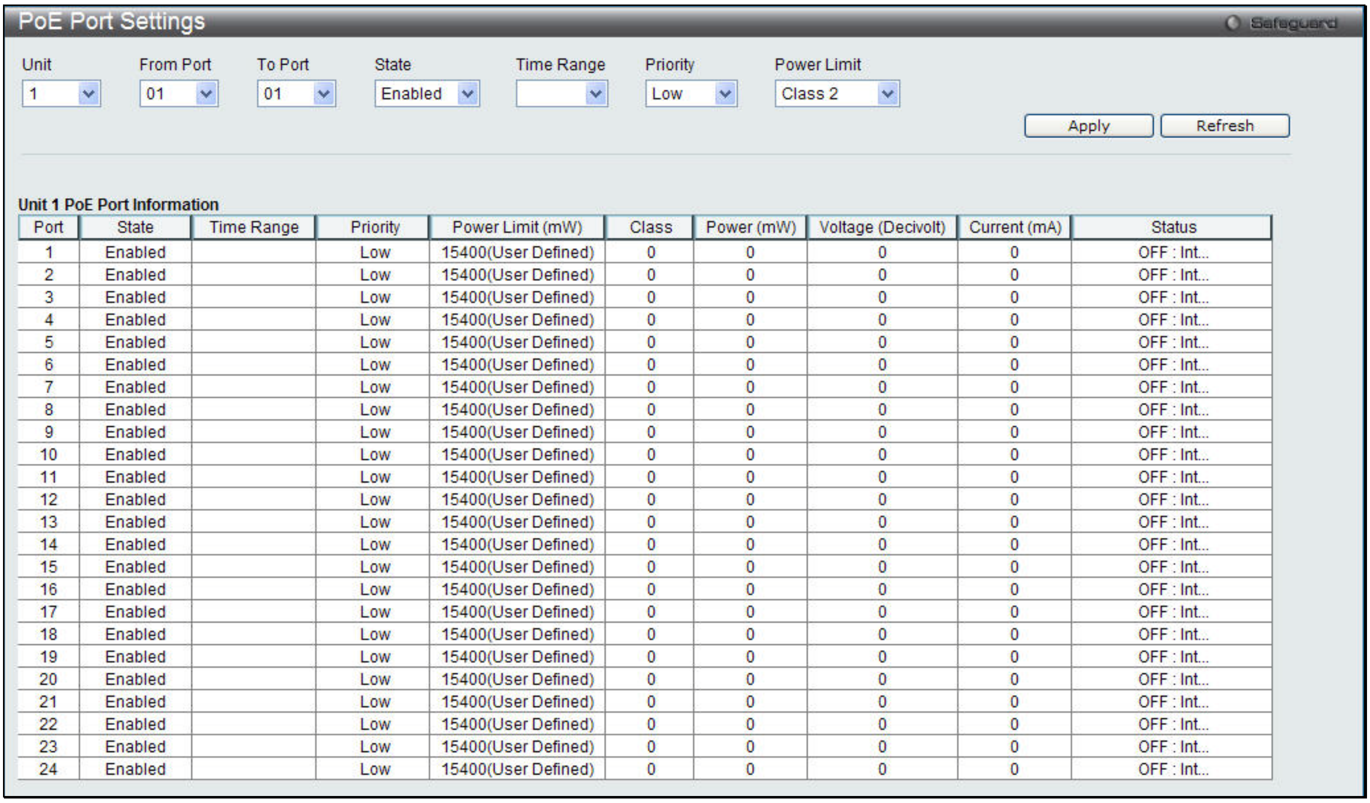
The following parameters can be configured:

Parameter	Description
Unit	Select the unit you wish to configure. Tick the **All** check box to select all units.
Power Limit (37-760)	Sets the limit of power to be used from the Switch's power source to PoE ports. The user may configure a Power Limit between 37W and 760W for the DGS-3120-24PC and DGS-3120-48PC. The default setting is 760W.
Power Disconnect Method	The PoE controller uses either *Deny Next Port* or *Deny Low Priority Port* to offset the power limit being exceeded and keeps the Switch's power at a usable level. Use the drop down menu to select a **Power Disconnect Method**. The default Power Disconnect Method is *Deny Next Port*. Both Power Disconnection Methods are described below: *Deny Next Port* – After the power limit has been exceeded, the next port attempting to power up is denied, regardless of its priority. If Power Disconnection Method is set to *Deny Next Port*, the system cannot utilize out of its maximum power capacity. The maximum unused watt is 19W. *Deny Low Priority Port* – After the power limit has been exceeded, the next port attempting to power up causes the port with the lowest priority to shut down so as to allow the high-priority and critical priority ports to power up.
Legacy PD	Use the drop-down menu to enable or disable detecting legacy PDs signal.

Click **Apply** to implement changes made.

PoE Port Settings

To view the following window, click **System Configuration > PoE > PoE Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
State: Enabled
Time Range:
Priority: Low
Power Limit: Class 2

Unit 1 PoE Port Information

Port	State	Time Range	Priority	Power Limit (mW)	Class	Power (mW)	Voltage (Decivolt)	Current (mA)	Status
1	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
2	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
3	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
4	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
5	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
6	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
7	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
8	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
9	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
10	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
11	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
12	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
13	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
14	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
15	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
16	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
17	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
18	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
19	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
20	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
21	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
22	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
23	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...
24	Enabled		Low	15400(User Defined)	0	0	0	0	OFF : Int...

Figure 2-8 PoE Port Settings window

The following parameters can be configured:

Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Select a range of ports from the drop-down menus to be enabled or disabled for PoE.
State	Use the drop-down menu to enable or disable ports for PoE.
Time Range	Select a range of the time to the port set as POE. If Time Range is configured, the power can only be supplied during the specified period of time.
Priority	Use the drop-down menu to select the priority of the PoE ports. Port priority determines the priority which the system attempts to supply the power to the ports. There are three levels of priority that can be selected, *Critical*, *High*, and *Low*. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the order of supplying power. Whether the disconnect method is set to deny low priority port, the priority of each port will be used by the system to manage the supply of power to ports.
Power Limit	This function is used to configure the per-port power limit. If a port exceeds its power limit, it will shut down. Based on 802.3af/802.3at, there are different PD classes and power consumption ranges; Class 0 – 0.44~15.4W Class 1 – 0.44~4.0W Class 2 – 4~7.0W Class 3 – 7~15.4W Class 4 – 15.4W The following is the power limit applied to the port for these five classes. For each class, the power limit is a little more than the power consumption range for that class. This

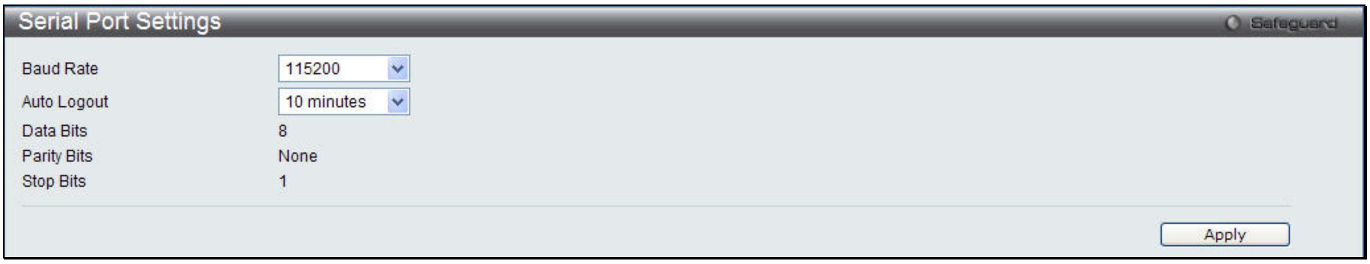
	takes into account any power loss on the cable. Thus, the following are the typical values; *Class 0* – 16200mW *Class 1* – 4200mW *Class 2* – 7400mW *Class 3* – 16200mW *User Define* – 35000mW

Click **Apply** to implement changes made. The port status of all PoE configured ports is displayed in the table in the bottom half of the screen shown above.

Serial Port Settings

This window allows the user to adjust the Baud Rate and the Auto Logout values.

To view the following window, click **System Configuration > Serial Port Settings**, as show below:



Baud Rate 115200

Auto Logout 10 minutes

Data Bits 8

Parity Bits None

Stop Bits 1

Figure 2-9 Serial Port Settings window

The fields that can be configured or displayed are described below:

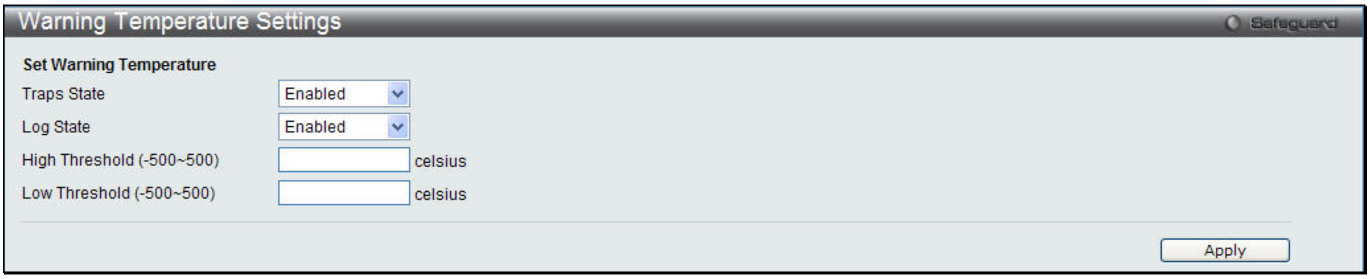
Parameter	Description
Baud Rate	Specify the baud rate for the serial port on the Switch. There are four possible baud rates to choose from, *9600*, *19200*, *38400* and *115200.* For a connection to the Switch using the console port, the baud rate must be set to *115200*, which is the default setting.
Auto Logout	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: *2, 5, 10, 15 minutes* or *Never*. The default setting is *10 minutes*.
Data Bits	Display the data bits used for the serial port connection.
Parity Bits	Display the parity bits used for the serial port connection.
Stop Bits	Display the stop bits used for the serial port connection.

Click the **Apply** button to implement changes made.

Warning Temperature Settings

This window allows the user to configure the system warning temperature parameters.

To view the following window, click **System Configuration > Warning Temperature Settings**, as show below:



Traps State Enabled

Log State Enabled

High Threshold (-500~500) celsius

Low Threshold (-500~500) celsius

Figure 2-10 Warning Temperature Settings window

The fields that can be configured are described below:

Parameter	Description
Traps State	Use the drop-down menu to enable or disable the traps state option of the warning temperature setting.
Log State	Use the drop-down menu to enable or disable the log state option of the warning temperature setting.
High Threshold	Enter the high threshold value of the warning temperature setting.
Low Threshold	Enter the low threshold value of the warning temperature setting.

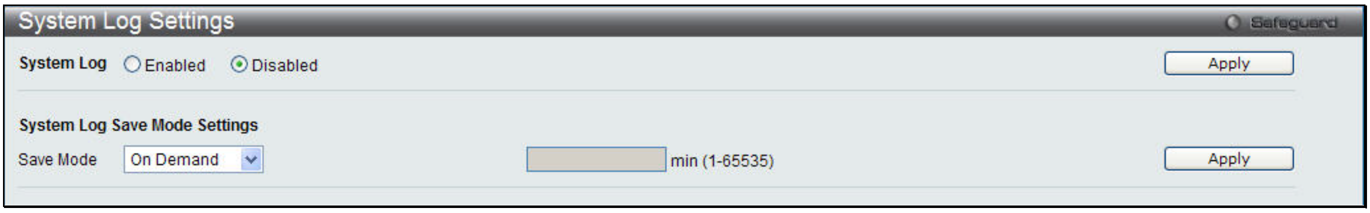
Click the **Apply** button to implement changes made.

System Log Configuration

System Log Settings

The Switch allows users to choose a method for which to save the switch log to the flash memory of the Switch.

To view the following window, click **System Configuration > System Log Configuration > System Log Settings**, as show below:



System Log ○ Enabled ● Disabled

System Log Save Mode Settings

Save Mode: On Demand

min (1-65535)

Figure 2-11 System Log Settings window

The fields that can be configured are described below:

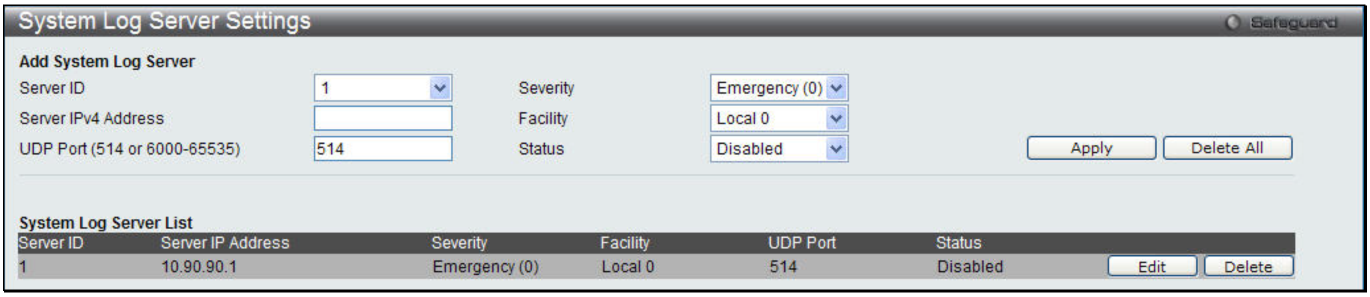
Parameter	Description
System Log	Use the radio buttons to enable or disable the system log settings.
Save Mode	Use the drop-down menu to choose the method for saving the switch log to the flash memory. The user has three options: *On Demand* – Users who choose this method will only save log files when they manually tell the Switch to do so, either using the Save Log link in the Save folder. *Time Interval* – Users who choose this method can configure a time interval by which the Switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes. *Log Trigger* – Users who choose this method will have log files saved to the Switch every time a log event occurs on the Switch.

Click the **Apply** button to accept the changes made for each individual section.

System Log Server Settings

The Switch can send System log messages to up to four designated servers using the System Log Server.

To view the following window, click **System Configuration > System Log Configuration > System Log Server Settings**, as show below:



Add System Log Server

Server ID: 1

Server IPv4 Address:

UDP Port (514 or 6000-65535): 514

Severity: Emergency (0)

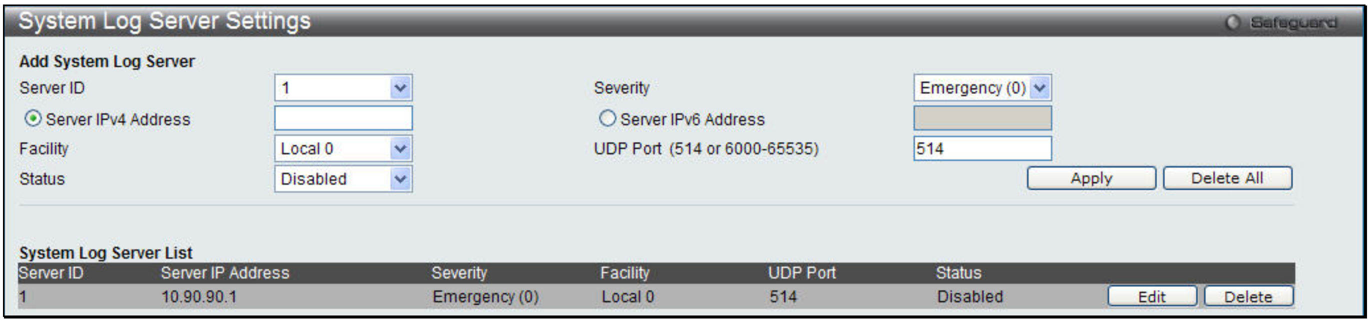
Facility: Local 0

Status: Disabled

System Log Server List

Server ID	Server IP Address	Severity	Facility	UDP Port	Status
1	10.90.90.1	Emergency (0)	Local 0	514	Disabled

Figure 2-12 System Log Server Settings (SI Mode Only)



Add System Log Server

Server ID: 1

● Server IPv4 Address:

○ Server IPv6 Address:

Facility: Local 0

Status: Disabled

Severity: Emergency (0)

UDP Port (514 or 6000-65535): 514

System Log Server List

Server ID	Server IP Address	Severity	Facility	UDP Port	Status
1	10.90.90.1	Emergency (0)	Local 0	514	Disabled

Figure 2-13 System Log Server Settings (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
Server ID	Syslog server settings index (1 to 4).
Severity	Use the drop-down menu to select the higher level of messages that will be sent. All messages which level is higher than selecting level will be sent. The options are *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Informational* and *Debug*.
Server IPv4 Address	The IPv4 address of the Syslog server.
Server IPv6 Address (EI Mode Only)	The IPv6 address of the Syslog server.
Facility	Use the drop-down menu to select *Local 0*, *Local 1*, *Local 2*, *Local 3*, *Local 4*, *Local 5*, *Local 6*, or *Local 7*.
UDP Port	Type the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose Enabled or Disabled to activate or deactivate.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

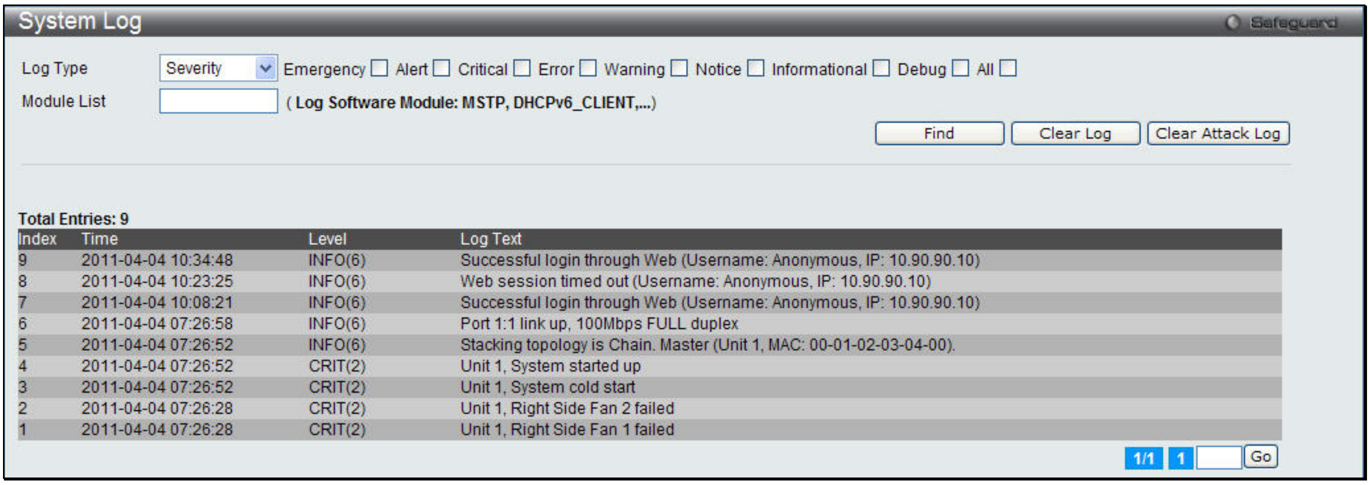
Click the **Delete** button to remove the specific entry.

Click the **Delete All** button to remove all servers configured.

System Log

Users can view and delete the local history log as compiled by the Switch's management agent.

To view the following window, click **System Configuration > System Log Configuration > System Log**, as show below:


System Log
Safeguard
Log Type
Severity
Emergency ☐ Alert ☐ Critical ☐ Error ☐ Warning ☐ Notice ☐ Informational ☐ Debug ☐ All ☐
Module List
(Log Software Module: MSTP, DHCPv6_CLIENT,...)
Find
Clear Log
Clear Attack Log
1/1
1
Go

Total Entries: 9

Index	Time	Level	Log Text
9	2011-04-04 10:34:48	INFO(6)	Successful login through Web (Username: Anonymous, IP: 10.90.90.10)
8	2011-04-04 10:23:25	INFO(6)	Web session timed out (Username: Anonymous, IP: 10.90.90.10)
7	2011-04-04 10:08:21	INFO(6)	Successful login through Web (Username: Anonymous, IP: 10.90.90.10)
6	2011-04-04 07:26:58	INFO(6)	Port 1:1 link up, 100Mbps FULL duplex
5	2011-04-04 07:26:52	INFO(6)	Stacking topology is Chain. Master (Unit 1, MAC: 00-01-02-03-04-00).
4	2011-04-04 07:26:52	CRIT(2)	Unit 1, System started up
3	2011-04-04 07:26:52	CRIT(2)	Unit 1, System cold start
2	2011-04-04 07:26:28	CRIT(2)	Unit 1, Right Side Fan 2 failed
1	2011-04-04 07:26:28	CRIT(2)	Unit 1, Right Side Fan 1 failed

Figure 2-14 System Log window

The fields that can be configured are described below:

Parameter	Description
Log Type	In the drop-down menu the user can select the log type that will be displayed. *Severity* - When selecting *Severity* from the drop-down menu, a secondary tick must be made. Secondary ticks are **Emergency, Alert, Critical, Error, Warning, Notice, Informational** and **Debug**. To view all information in the log, simply tick the **All** check box. *Module List* - When selecting *Module List*, the module name must be manually entered. Available modules are MSTP, ERROR_LOG, CFM_EXT, and ERPS. *Attack Log* - When selecting *Attack Log* all attacks will be listed.
Index	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Display the time in days, hours, minutes, and seconds since the Switch was last restarted.
Level	Display the level of the log entry.
Log Text	Display text describing the event that triggered the history log entry.

Click the **Find** button to display the log in the display section according to the selection made.

Click the **Clear Log** button to clear the entries from the log in the display section.

Click the **Clear Attack Log** button to clear the entries from the attack log in the display section.

The Switch can record event information in its own log. Click **Go** to go to the next page of the **System Log** window.

System Log & Trap Settings

The Switch allows users to configure the system log source IP interface addresses here.

To view the following window, click **System Configuration > System Log Configuration > System Log & Trap Settings**, as show below:

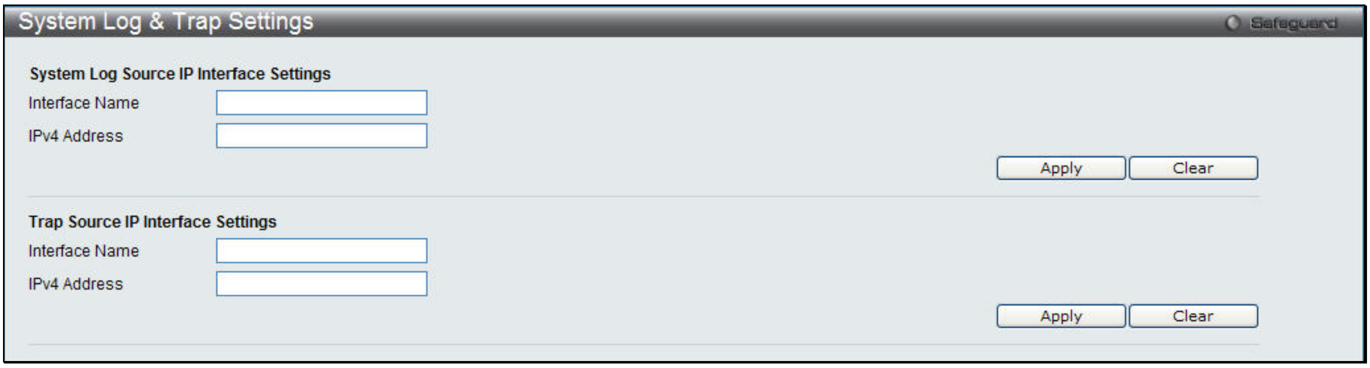

System Log & Trap Settings
Safeguard
System Log Source IP Interface Settings
Interface Name
IPv4 Address
Apply
Clear
Trap Source IP Interface Settings
Interface Name
IPv4 Address
Apply
Clear

Figure 2-15 System Log & Trap Settings window (SI Mode Only)

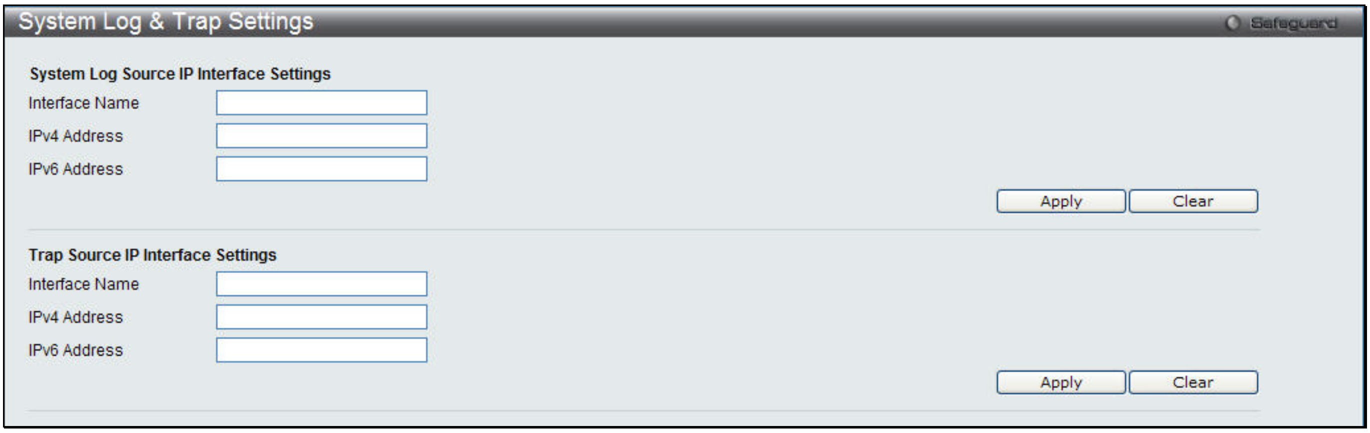

System Log & Trap Settings
Safeguard
System Log Source IP Interface Settings
Interface Name
IPv4 Address
IPv6 Address
Apply
Clear
Trap Source IP Interface Settings
Interface Name
IPv4 Address
IPv6 Address
Apply
Clear

Figure 2-16 System Log & Trap Settings window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the IP interface name used.
IPv4 Address	Enter the IPv4 address used.
IPv6 Address (EI Mode Only)	Enter the IPv6 address used.

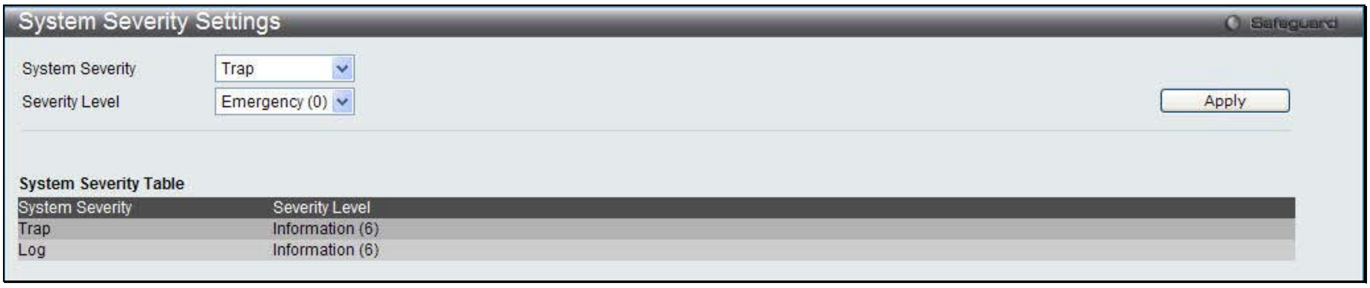
Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all the information entered in the fields.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent. The level at which the alert triggers either a log entry or a trap message can be set as well. Use the System Severity Settings window to set the criteria for alerts. The current settings are displayed below the System Severity Table.

To view the following window, click **System Configuration > System Log Configuration > System Severity Settings**, as show below:


System Severity Settings
Safeguard
Apply

System Severity: Trap
Severity Level: Emergency (0)

System Severity Table

System Severity	Severity Level
Trap	Information (6)
Log	Information (6)

Figure 2-17 System Severity Settings window

The fields that can be configured are described below:

Parameter	Description
System Severity	Choose how the alerts are used from the drop-down menu. Select *Log* to send the alert of the Severity Type configured to the Switch's log for analysis. Choose *Trap* to send it to an SNMP agent for analysis, or select *All* to send the chosen alert type to an SNMP agent and the Switch's log for analysis.
Severity Level	This drop-down menu allows you to select the level of messages that will be sent. The options are *Emergency (0), Alert (1), Critical (2), Error (3), Warning (4), Notice (5), Information (6)* and *Debug (7).*

Click the **Apply** button to accept the changes made.

Time Range Settings

Time range is a time period that the respective function will take an effect on, such as ACL. For example, the administrator can configure the time-based ACL to allow users to surf the Internet on every Saturday and every Sunday, meanwhile to deny users to surf the Internet on weekdays.

The user may enter up to 64 time range entries on the Switch.

To view the following window, click **System Configuration > Time Range Settings**, as show below:

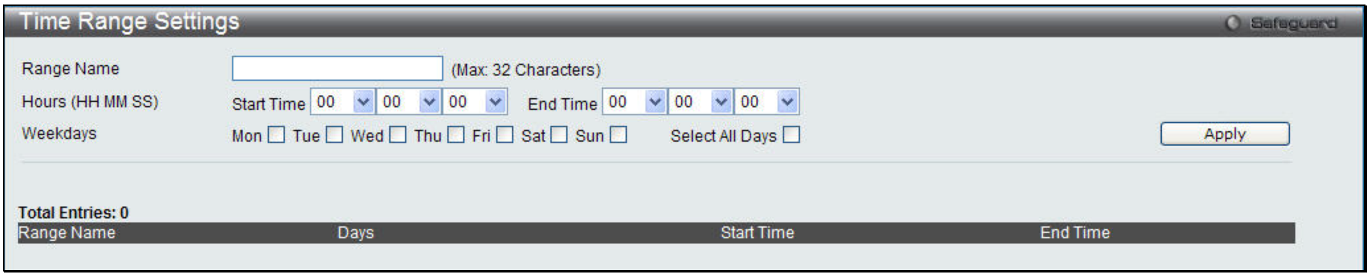

Time Range Settings
Safeguard
Range Name
(Max: 32 Characters)
Hours (HH MM SS)
Start Time 00 00 00
End Time 00 00 00
Weekdays
Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun ☐
Select All Days ☐
Apply
Total Entries: 0
Range Name
Days
Start Time
End Time

Figure 2-18 Time Range Settings window

The fields that can be configured are described below:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile table to identify the access profile and associated rule to be enabled during this time range.
Hours	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: *Start Time* - Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. *End Time* - Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Tick the Select All Days check box to configure this time range for every day of the week.

Click the **Apply** button to accept the changes made. Current configured entries will be displayed in the **Time Range Information** table in the bottom half of the window shown above.

Port Group Settings (EI Mode Only)

This window is used to create port groups, and add or delete ports from the port groups.

To view the following window, click **System Configuration > Port Group Settings**, as show below:

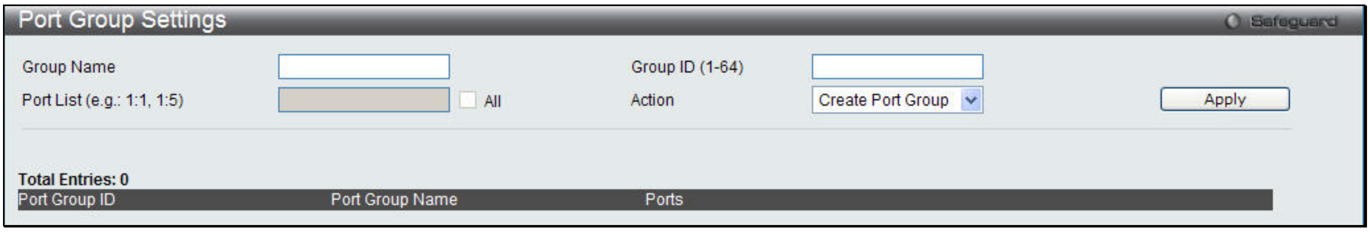

Port Group Settings
Safeguard
Group Name
Group ID (1-64)
Port List (e.g.: 1:1, 1:5)
☐ All
Action
Create Port Group
Apply
Total Entries: 0
Port Group ID
Port Group Name
Ports

Figure 2-19 Port Group Settings window

The fields that can be configured are described below:

Parameter	Description
Group Name	Enter the name of a port group.
Group ID (1-64)	Enter the ID of a port group
Port List	Enter a port or list of ports. Tick the **All** check box to apply to all ports.
Action	Use the drop-down menu to select *Create Port Group*, *Add Ports* or *Delete Ports*.

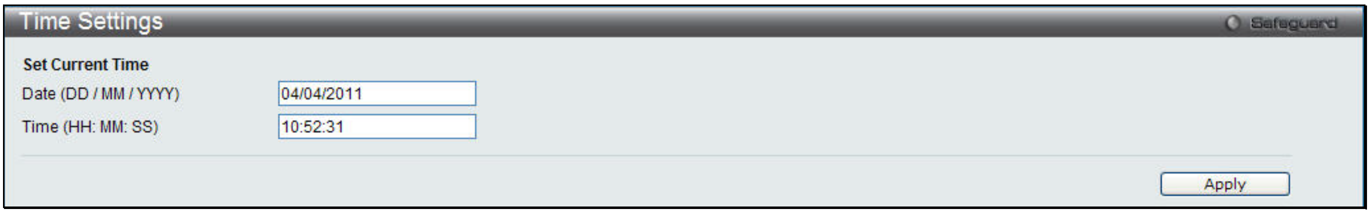
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Time Settings

Users can configure the time settings for the Switch.

To view the following window, click **System Configuration > Time Settings**, as show below:



Date (DD / MM / YYYY) 04/04/2011
Time (HH: MM: SS) 10:52:31

Figure 2-20 Time Settings window

The fields that can be configured are described below:

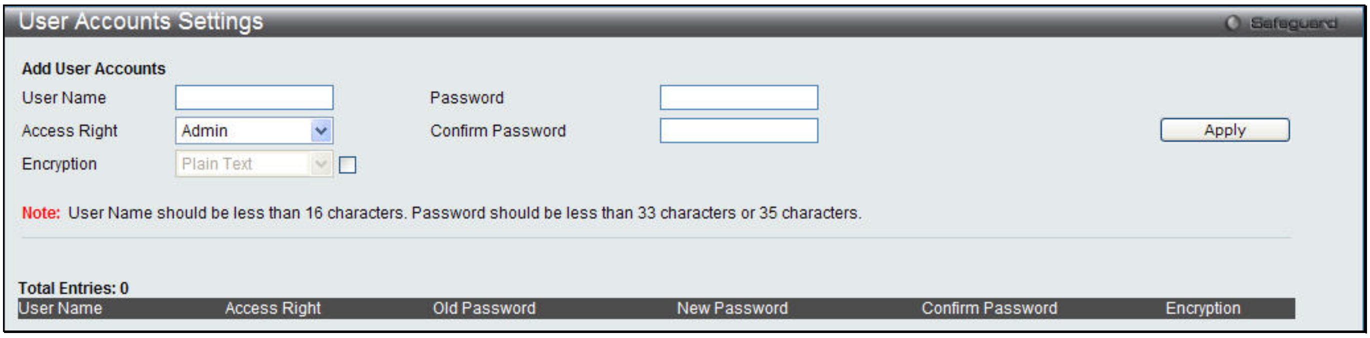
Parameter	Description
Date (DD/MM/YYYY)	Enter the current day, month, and year to update the system clock.
Time (HH:MM:SS)	Enter the current time in hours, minutes, and seconds.

Click the **Apply** button to accept the changes made.

User Accounts Settings

The Switch allows the control of user privileges.

To view the following window, click **System Configuration > User Accounts Settings**, as show below:



Access Right Admin
Encryption Plain Text ☐

Note: User Name should be less than 16 characters. Password should be less than 33 characters or 35 characters.

Total Entries: 0

User Name	Access Right	Old Password	New Password	Confirm Password	Encryption

Figure 2-21 User Accounts Settings window

To add a new user, type in a User Name and New Password and retype the same password in the Confirm New Password field. Choose the level of privilege (Admin, Operator, Power User or User) from the Access Right drop-down menu.

Management	Admin	Operator	Power User	User
Configuration	Read/Write	Read/Write–partly	Read/Write–partly	No
Network Monitoring	Read/Write	Read/Write	Read-only	Read-only
Community Strings and Trap Stations	Read/Write	Read-only	Read-only	Read-only
Update Firmware and Configuration Files	Read/Write	Read/Write	No	No
System Utilities	Read/Write	Read-only	Read-only	Read-only
Factory Reset	Read/Write	No	No	No
User Account Management				
Add/Update/Delete User Accounts	Read/Write	No	No	No
View User Accounts	Read/Write	No	No	No

The fields that can be configured are described below:

Parameter	Description
User Name	Enter a new user name for the Switch.
Password	Enter a new password for the Switch.
Confirm Password	Re-type in a new password for the Switch.
Access Right	Specify the access right for this user.
Encryption	Specifies that encryption will be applied to this account. Option to choose from are *Plain Text*, and *SHA-1*.

Click the **Apply** button to accept the changes made.

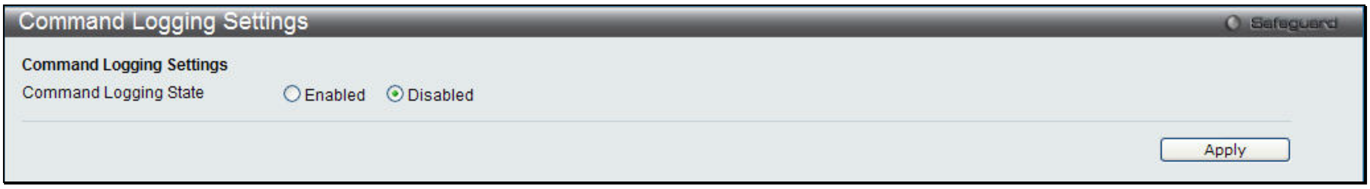
NOTICE: In case of lost passwords or password corruption, please refer to the appendix chapter entitled, “Password Recovery Procedure,” which will guide you through the steps necessary to resolve this issue.

NOTE: The username and password should be less than 16 characters.

Command Logging Settings

This window is used to enable or disable the command logging settings.

To view this window, click **System Configuration** > **Command Logging Settings**, as shown below:



Command Logging Settings

Command Logging State ○ Enabled ● Disabled

Figure 2-22 Command Logging Settings window

The fields that can be configured are described below:

Parameter	Description
Command Logging State	Use the radio buttons to enable or disable the function.

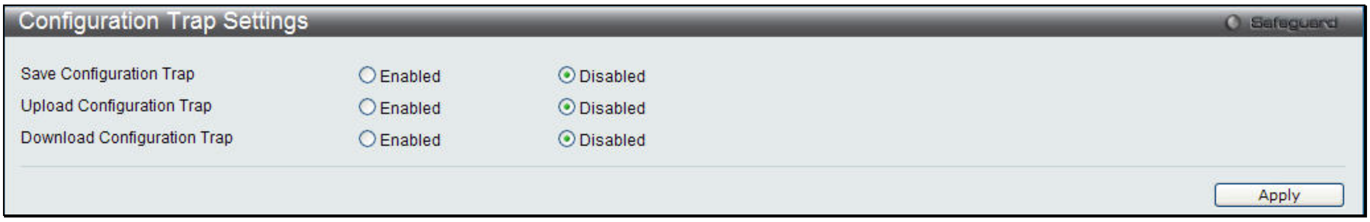
Click the **Apply** button to accept the changes made.

NOTE: When the switch is under the booting procedure, all configuration commands will not be logged. When the user uses AAA authentication to logged in, the user name should not be changed if the user has used the Enable Admin function to replace its privilege.

Configuration Trap Settings

This window is used to configure the trap settings when the configuration is saved, uploaded and downloaded.

To view this window, click **System Configuration** > **Configuration Trap Settings**, as shown below:



Save Configuration Trap ○ Enabled ● Disabled
Upload Configuration Trap ○ Enabled ● Disabled
Download Configuration Trap ○ Enabled ● Disabled

Figure 2-23 Configuration Trap Settings window

The fields that can be configured are described below:

Parameter	Description
Save Configuration Trap	Use the drop-down menu to enable or disable sending the trap by the SNMP agent when the configuration is saved in NVRAM.
Upload configuration Trap	Use the drop-down menu to enable or disable sending the trap by the SNMP agent when successfully uploading configuration.
Download Configuration Trap	Use the drop-down menu to enable or disable sending the trap by the SNMP agent when successfully downloading configuration.

Click the **Apply** button to accept the changes made.

Stacking

From firmware release v1.00 of this Switch, the Switch now supports switch stacking, where a set of six switches can be combined to be managed by one IP address through Telnet, the GUI interface (web), the console port or through SNMP. Each switch of this series has two stacking ports located at the rear of the device, which can be used to connect other devices and make them stack together. After adding these stacking ports, the user may connect these ports together using copper cables (also sold separately) in one of two possible topologies.

Duplex Chain – As shown in Figure 2-25, The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.

Duplex Ring – As shown in Figure 2-26, the Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient due to the fact that if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

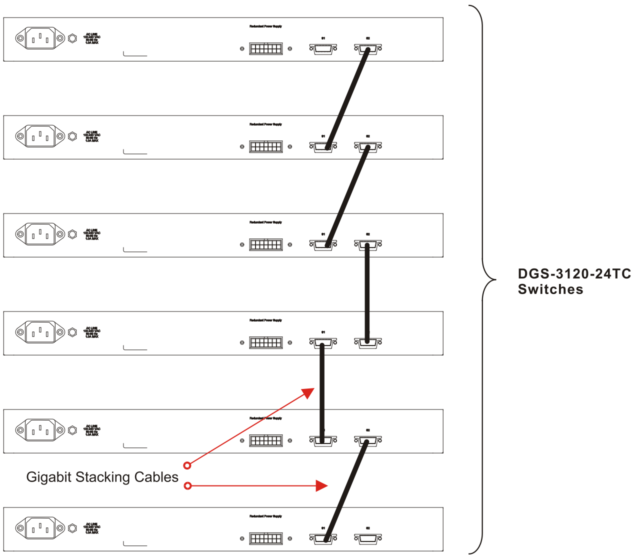


Figure 2-24 Switches stacked in a Duplex Chain

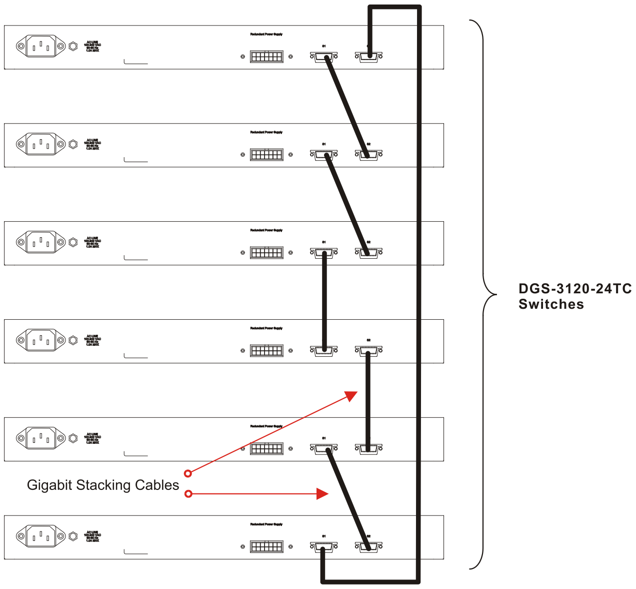


Figure 2-25 Switches stacked in a Duplex Ring

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the Switch stack. Three possible roles exist when stacking with the Switch.

Primary Master – The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining switches in the switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the lowest MAC address and then will assign that switch as the Primary Master, if all priorities are the same. The Primary master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and ‘H’.

Backup Master – The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same. The Backup master are physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and ‘h’.

Slave – Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology and adhere to the Backup Master’s commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State – This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State – Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State – Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the users configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the Switch supports “hot swapping” of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are “hot inserted” into the running stack, the new switch may take on the Primary Master, Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master’s roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The “hot remove” action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master’s role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

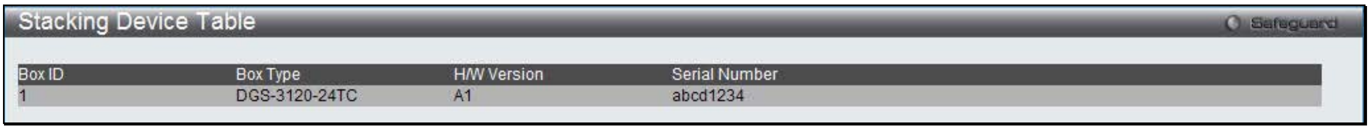
If both the Primary Master and the Backup Master are removed, the election process is immediately processed and a new Primary Master and Backup Master is determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.

NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

Stacking Device Table

This window is used to display the current devices in the Switch Stack.

To view this window, click **System Configuration > Stacking > Stacking Device Table**, as shown below:



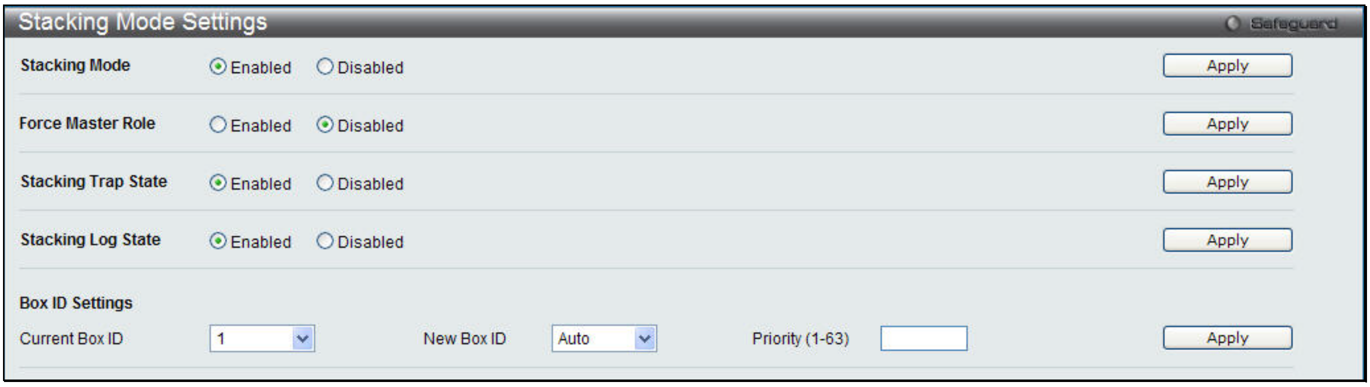
Box ID	Box Type	H/W Version	Serial Number
1	DGS-3120-24TC	A1	abcd1234

Figure 2-26 Stacking Device Table window

Stacking Mode Settings

To begin the stacking process, users must first enable this device for stacking by using the Stacking Mode Settings window.

To view this window, click **System Configuration > Stacking > Stacking Mode Settings**, as shown below:



Stacking Mode ● Enabled ○ Disabled

Force Master Role ○ Enabled ● Disabled

Stacking Trap State ● Enabled ○ Disabled

Stacking Log State ● Enabled ○ Disabled

Box ID Settings

Current Box ID: 1 New Box ID: Auto Priority (1-63):

Figure 2-27 Stacking Mode Settings window

The fields that can be configured or viewed are described below:

Parameter	Description
Stacking Mode	Specifies whether the stacking mode feature will be enabled or disabled. When enabled, the 10Gb ports will function as stacking ports. When disabled, the 10Gb ports will return to normal 10Gb XFP module ports.
Force Master Role	Use the radio buttons to enable or disable the function. It is used to ensure the master role is unchanged when adding a new device to the current stacking topology. If the **Enabled** radio button is selected, the master's priority will become zero after the stacking has stabilized.
Stacking Trap State	Click the radio buttons to enable or disable sending the trap for stacking.
Stacking Log State	Click the radio buttons to enable or disable logging the stacking log.
Current Box ID	The Box ID of the switch in the stack to be configured.
New Box ID	The new box ID of the selected switch in the stack that was selected in the Current Box ID field. The user may choose any number between 1 and 6 to identify the switch in the switch stack. *Auto* will automatically assign a box number to the switch in the switch stack.
Priority (1-63)	Displays the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack is the Primary Master switch. The Primary Master switch will be used to configure applications of the switch stack.

Click the **Apply** button to accept the changes made.

Chapter 3 Management

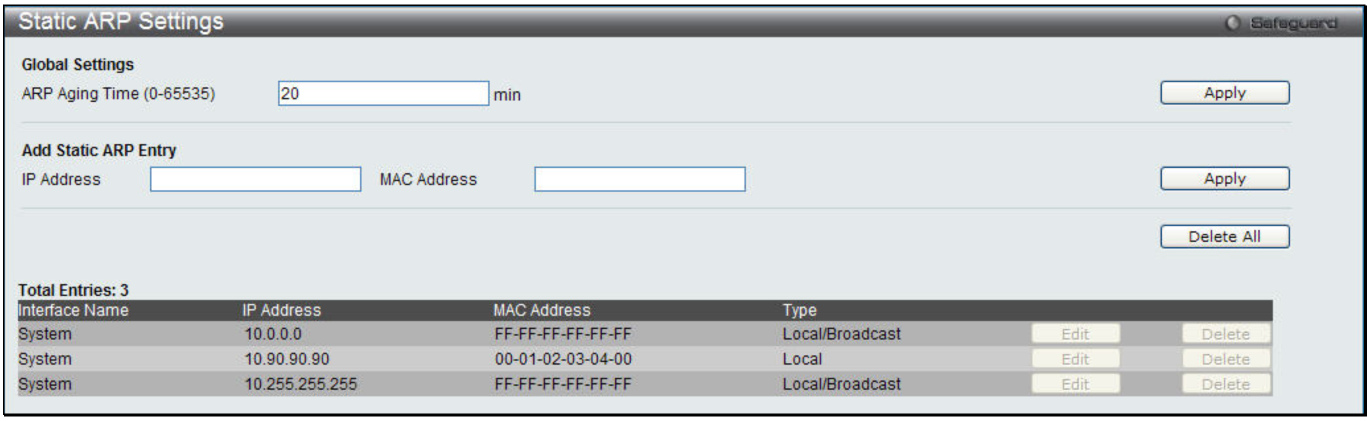
ARP
Gratuitous ARP
IPv6 Neighbor Settings (EI Mode Only)
IP Interface
Management Settings
Session Table
Single IP Management
SNMP Settings
Telnet Settings
Web Settings
Power Saving
SD Card Management

ARP

Static ARP Settings

The Address Resolution Protocol is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify, and delete ARP information for specific devices. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

To view the following window, click **Management > ARP > Static ARP Settings**, as show below:



ARP Aging Time (0-65535): 20 min

Total Entries: 3

Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.90.90.90	00-01-02-03-04-00	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

Figure 3-1 Static ARP Settings window

The fields that can be configured are described below:

Parameter	Description
ARP Aging Time (0-65535)	The ARP entry age-out time, in minutes. The default is *20* minutes.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

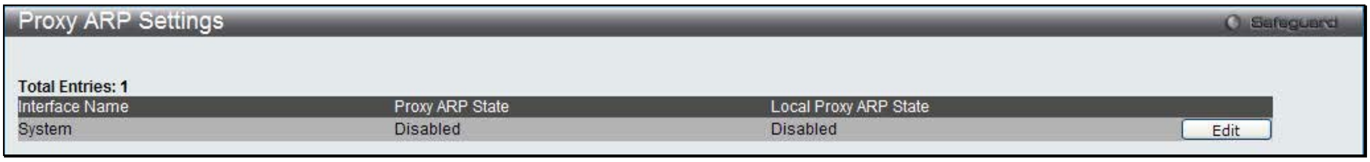
Proxy ARP Settings (EI Mode Only)

The Proxy ARP (Address Resolution Protocol) feature of the Switch will allow the Switch to reply to ARP requests destined for another device by faking its identity (IP and MAC Address) as the original ARP responder. Therefore, the Switch can then route packets to the intended destination without configuring static routing or a default gateway.

The host, usually a layer 3 switch, will respond to packets destined for another device. For example, if hosts A and B are on different physical networks, B will not receive ARP broadcast requests from A and therefore cannot respond. Yet, if the physical network of A is connected by a router or layer 3 switch to B, the router or Layer 3 switch will see the ARP request from A.

This local proxy ARP function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.

To view the following window, click **Management > ARP > Proxy ARP Settings**, as show below:



Total Entries: 1

Interface Name	Proxy ARP State	Local Proxy ARP State
System	Disabled	Disabled

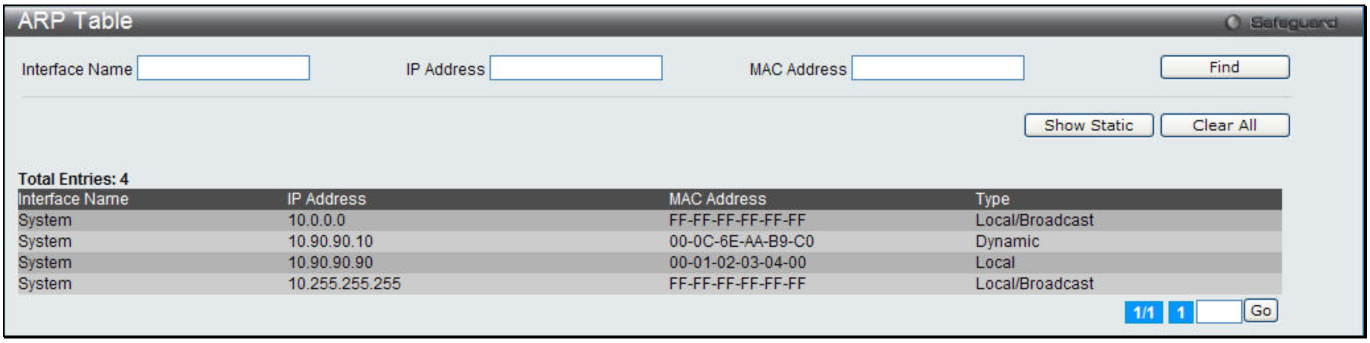
Figure 3-2 Proxy ARP Settings window

Click the **Edit** button to re-configure the specific entry and select the proxy ARP state of the IP interface. By default, both the **Proxy ARP State** and **Local Proxy ARP State** are disabled.

ARP Table

Users can display current ARP entries on the Switch.

To view the following window, click **Management > ARP > ARP Table**, as show below:



Total Entries: 4

Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.90.90.10	00-0C-6E-AA-B9-C0	Dynamic
System	10.90.90.90	00-01-02-03-04-00	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

Figure 3-3 ARP Table window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter or view the Interface name used.
IP Address	Enter or view the IP Address used.
MAC Address	Enter or view the MAC Address used.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show Static** button to display only the static entries in the display table.

Click the **Clear All** button to remove all the entries listed in the table.

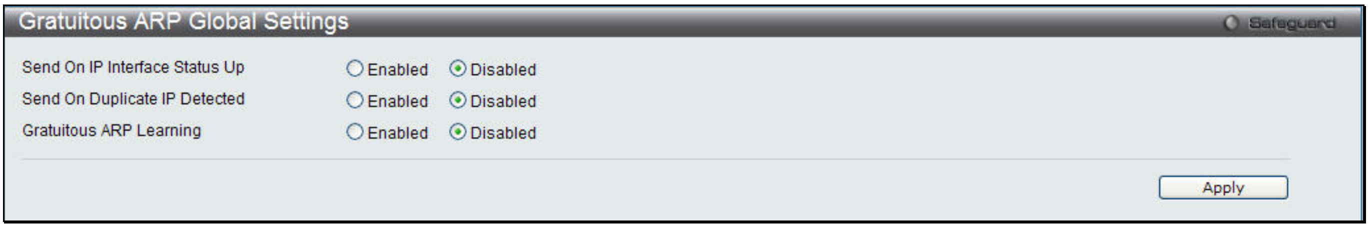
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Gratuitous ARP

Gratuitous ARP Global Settings

The user can enable or disable the gratuitous ARP global settings here.

To view the following window, click **Management > Gratuitous ARP > Gratuitous ARP Global Settings**, as show below:



Send On IP Interface Status Up ○ Enabled ● Disabled
Send On Duplicate IP Detected ○ Enabled ● Disabled
Gratuitous ARP Learning ○ Enabled ● Disabled

Figure 3-4 Gratuitous ARP Global Settings Window

The fields that can be configured are described below:

Parameter	Description
Send On IP Interface Status Up	The command is used to enable/disable sending of gratuitous ARP request packet while the IPIF interface become up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled, and only one gratuitous ARP packet will be broadcast.
Send On Duplicate IP Detected	The command is used to enable/disable the sending of gratuitous ARP request packet while a duplicate IP is detected. By default, the state is disabled. For this command, the duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that match the system's own IP address. In this case, the system knows that somebody out there uses an IP address that is conflict with the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packets for this duplicate IP address.
Gratuitous ARP Learning	Normally, the system will only learn the ARP reply packet or a normal ARP request packet that asks for the MAC address that corresponds to the system's IP address. The command is used to enable/disable learning of ARP entry in ARP cache based on the received gratuitous ARP packet. The gratuitous ARP packet is sent by a source IP address that is identical to the IP that the packet is queries for. By default, the state is Disabled status.

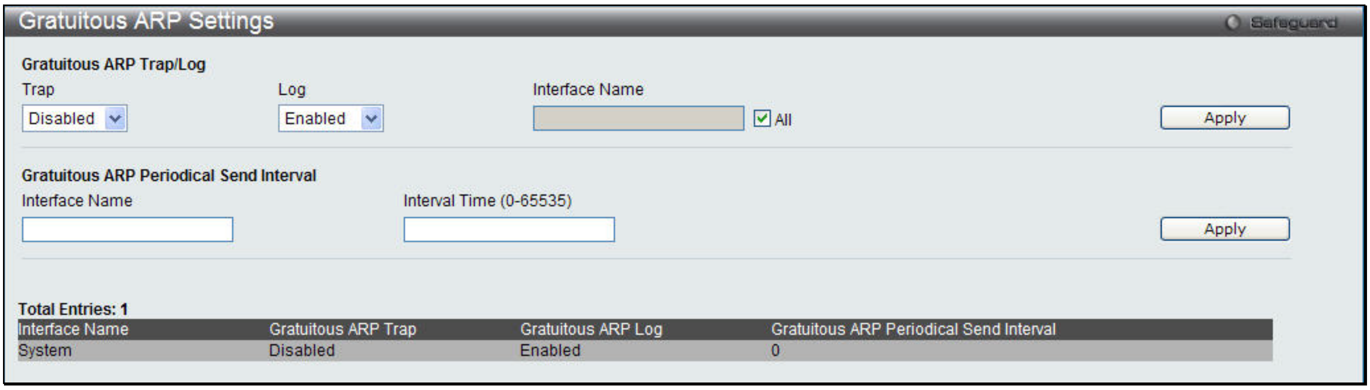
Click the **Apply** button to accept the changes made.

NOTE: With the gratuitous ARP learning, the system will not learn new entry but only do the update on the ARP table based on the received gratuitous ARP packet.

Gratuitous ARP Settings

The user can configure the IP interface's gratuitous ARP parameter.

To view the following window, click **Management > Gratuitous ARP > Gratuitous ARP Settings**, as show below:



Gratuitous ARP Trap/Log

Trap: Disabled

Log: Enabled

Interface Name: ☑ All

Gratuitous ARP Periodical Send Interval

Interface Name:

Interval Time (0-65535):

Total Entries: 1

Interface Name	Gratuitous ARP Trap	Gratuitous ARP Log	Gratuitous ARP Periodical Send Interval
System	Disabled	Enabled	0

Figure 3-5 Gratuitous ARP Settings window

The fields that can be configured are described below:

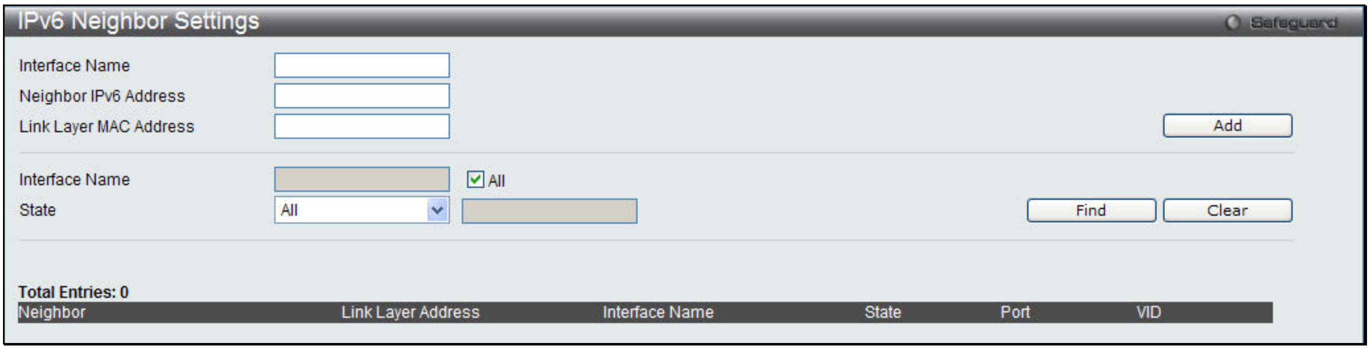
Parameter	Description
Trap	Use the drop-down menu to enable or disable the trap option. By default the trap is disabled.
Log	Use the drop-down menu to enable or disable the logging option. By default the event log is enabled.
Interface Name	Enter the interface name of the Layer 3 interface. Select **All** to enable or disable gratuitous ARP trap or log on all interfaces.
Interval Time (0-65535)	Enter the periodically send gratuitous ARP interval time in seconds. 0 means that gratuitous ARP request will not be sent periodically. By default the interval time is 0.

Click the **Apply** button to accept the changes made for each individual section.

IPv6 Neighbor Settings (EI Mode Only)

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

To view the following window, click **Management > IPv6 Neighbor Settings**, as show below:



Interface Name:

Neighbor IPv6 Address:

Link Layer MAC Address:

Interface Name: ☑ All

State: All

Total Entries: 0

Neighbor	Link Layer Address	Interface Name	State	Port	VID

Figure 3-6 IPv6 Neighbor Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the interface name of the IPv6 neighbor.
Neighbor IPv6 Address	Enter the neighbor IPv6 address.
Link Layer MAC Address	Enter the link layer MAC address.
Interface Name	Enter the name of the IPv6 neighbor. Tick the **All** check box to search for all current interfaces on the Switch.

State	Use the drop-down menu to select All, Address, Static, or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information entered in the fields.

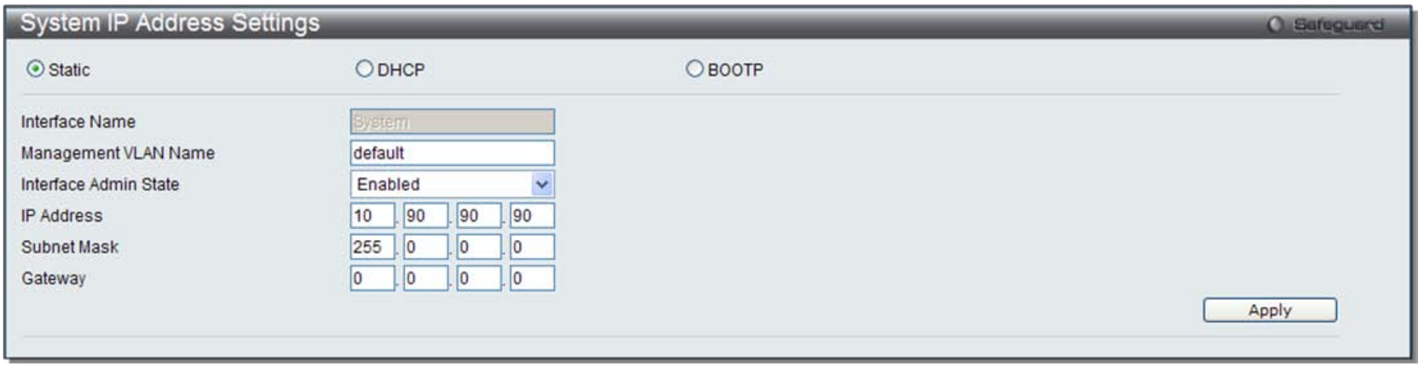
IP Interface

System IP Address Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. The Web manager will display the Switch’s current IP settings.

NOTE: The Switch’s factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To view the following window, click **Management > IP Interface > System IP Address Settings**, as show below:



● Static ○ DHCP ○ BOOTP

Interface Name: System
Management VLAN Name: default
Interface Admin State: Enabled
IP Address: 10 . 90 . 90 . 90
Subnet Mask: 255 . 0 . 0 . 0
Gateway: 0 . 0 . 0 . 0

Figure 3-7 System IP Address Settings window

The fields that can be configured are described below:

Parameter	Description
Static	Allow the entry of an IP address, subnet mask, and a default gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between *0* and *255*. This address should be a unique address on the network assigned for use by the network administrator.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

The following table will describe the fields that are about the **System** Interface.

Parameter	Description

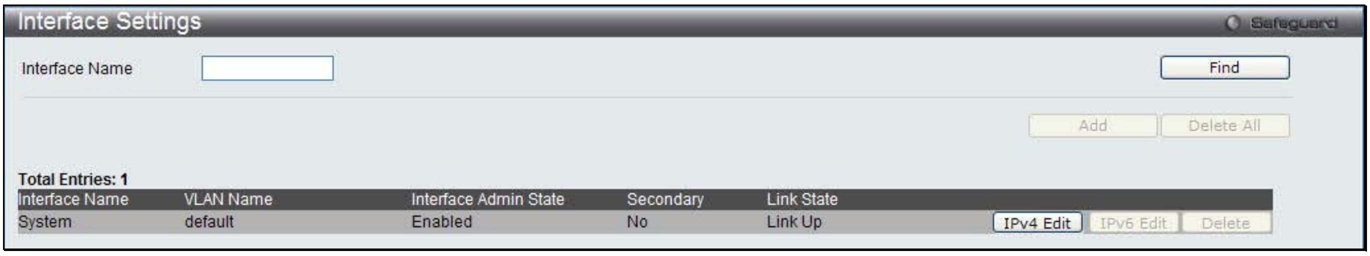
Interface Name	Display the System interface name.
Management VLAN Name	This allows the entry of a VLAN name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via Web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the **Trusted Host** window (**Security > Trusted Host)**. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Trusted Host table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP addresses are assigned.
Interface Admin State	Use the drop-down menu to enable or disable the configuration on this interface. If the state is disabled, the IP interface cannot be accessed.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between *0* and *255*. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

Click the **Apply** button to accept the changes made.

Interface Settings

Users can display the Switch's current IP interface settings.

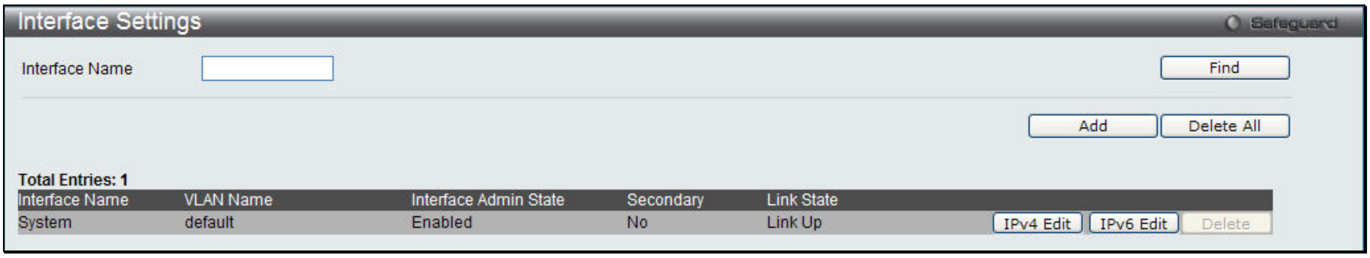
To view the following window, click **Management > IP Interface > Interface Settings**, as show below:



Total Entries: 1

Interface Name	VLAN Name	Interface Admin State	Secondary	Link State
System	default	Enabled	No	Link Up

Figure 3-8 Interface Settings window (SI Mode Only)



Total Entries: 1

Interface Name	VLAN Name	Interface Admin State	Secondary	Link State
System	default	Enabled	No	Link Up

Figure 3-9 Interface Settings window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IP interface to search for.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **IPv4 Edit** button to edit the IPv4 settings for the specific entry.

Click the **Add** button to add a new entry based on the information entered. **(EI Mode Only)**

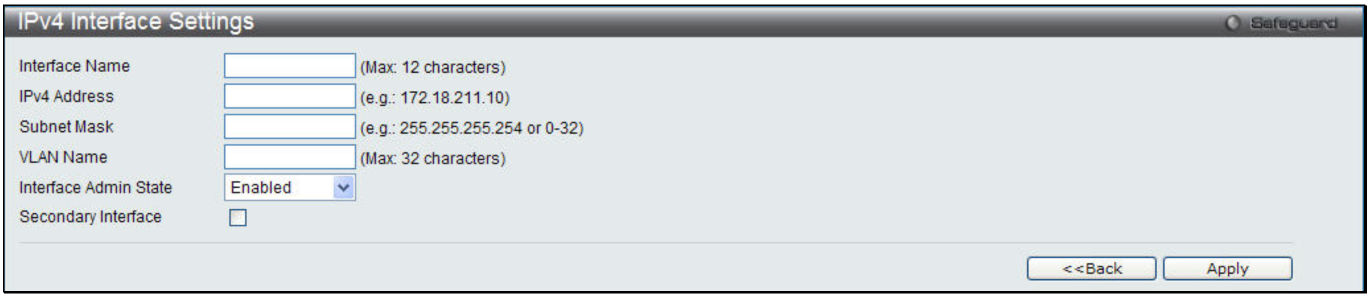
Click the **Delete All** button to remove all the entries listed. **(EI Mode Only)**

Click the **IPv6 Edit** button to edit the IPv6 settings for the specific entry. **(EI Mode Only)**

Click the **Delete** button to remove the specific entry. **(EI Mode Only)**

NOTE: To create IPv6 interfaces, the user has to create an IPv4 interface then edit it to IPv6.

Click the **Add** button to see the following window.



IPv4 Interface Settings

Interface Name (Max: 12 characters)
IPv4 Address (e.g.: 172.18.211.10)
Subnet Mask (e.g.: 255.255.255.254 or 0-32)
VLAN Name (Max: 32 characters)
Interface Admin State: Enabled
Secondary Interface ☐

Figure 3-10 IPv4 Interface Settings window (EI Mode Only)

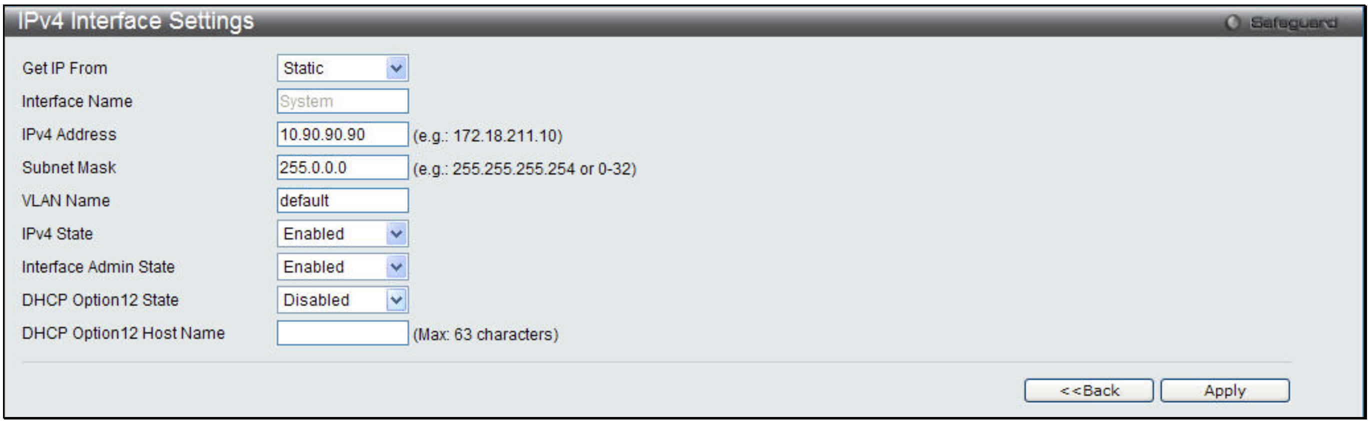
The fields that can be configured are described below:

Parameter	Description
IP Interface Name	Enter the name of the IP interface being created.
IPv4 Address	Enter the IPv4 address used.
Subnet Mask	Enter the IPv4 subnet mask used.
VLAN Name	Enter the VLAN Name used.
Interface Admin State	Use the drop-down menu to enable or disable the Interface Admin State.
Secondary Interface	Tick the check box to use this Interface as a Secondary Interface. When the primary IP is not available, the VLAN will switch to the secondary interface. It will switch back when the primary IP was recovered.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **IPv4 Edit** button to see the following window.



IPv4 Interface Settings

Get IP From: Static
Interface Name: System
IPv4 Address: 10.90.90.90 (e.g.: 172.18.211.10)
Subnet Mask: 255.0.0.0 (e.g.: 255.255.255.254 or 0-32)
VLAN Name: default
IPv4 State: Enabled
Interface Admin State: Enabled
DHCP Option12 State: Disabled
DHCP Option12 Host Name (Max: 63 characters)

Figure 3-11 IPv4 Interface Settings – Edit window

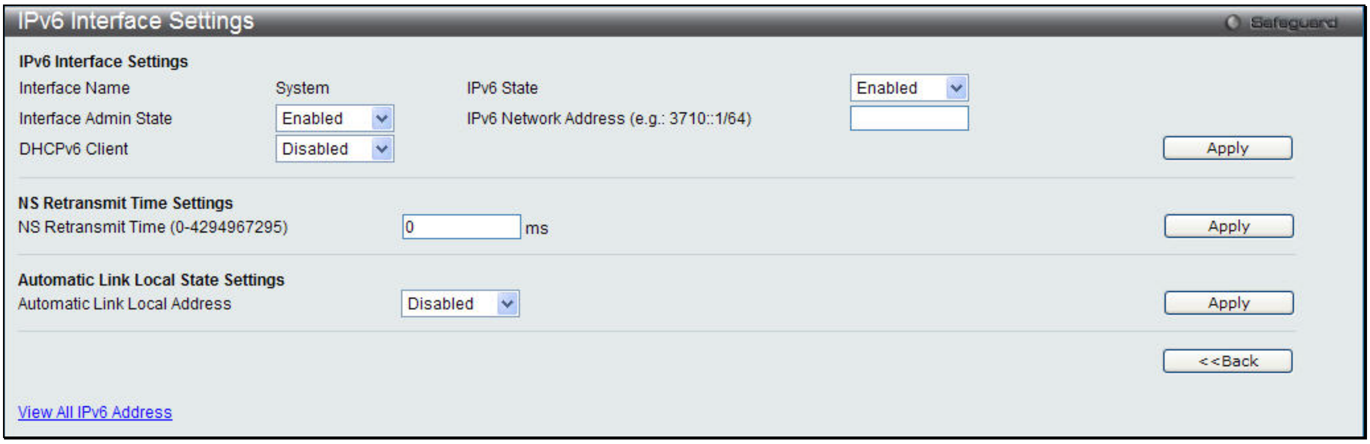
The fields that can be configured are described below:

Parameter	Description
Get IP From	Use the drop-down menu to specify the method that this Interface uses to acquire an IP address.
Interface Name	Enter the name of the IP interface being configured.
IPv4 Address	Enter the IPv4 address used.
Subnet Mask	Enter the IPv4 subnet mask used.
VLAN Name	Enter the VLAN Name used.
IPv4 State	Use the drop-down menu to enable or disable IPv4 State.
Interface Admin State	Use the drop-down menu to enable or disable the Interface Admin State.
DHCP Option 12 State	Use the drop-down menu to enable or disable insertion of option 12 in the DHCPDISCOVER and DHCPREQUEST message.
DHCP Option 12 Host Name	Enter the host name to be inserted in the DHCPDISCOVER and DHCPREQUEST message.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **IPv6 Edit** button to see the following window.



IPv6 Interface Settings

Interface Name: System

IPv6 State: Enabled

Interface Admin State: Enabled

IPv6 Network Address (e.g.: 3710::1/64):

DHCPv6 Client: Disabled

NS Retransmit Time Settings

NS Retransmit Time (0-4294967295): 0 ms

Automatic Link Local State Settings

Automatic Link Local Address: Disabled

Figure 3-12 IPv6 Interface Settings window (EI Mode Only)

The fields that can be configured or displayed are described below:

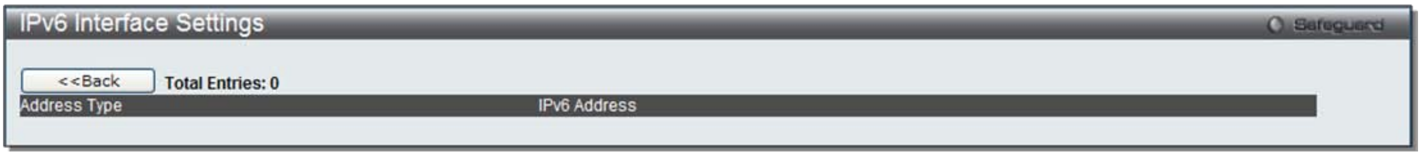
Parameter	Description
Interface Name	Display the IPv6 interface name.
IPv6 State	Use the drop-down menu to enable or disable IPv6 State.
Interface Admin State	Use the drop-down menu to enable or disable the Interface Admin State.
IPv6 Network Address	Here the user can enter the neighbor’s global or local link address.
DHCPv6 Client	Use the drop-down menu to enable or disable DHCPv6 client.
NS Retransmit Time	Enter the Neighbor solicitation’s retransmit timer in millisecond here. It has the same value as the RA retransmit time in the config ipv6 nd ra command. If this field is configured, it will duplicate the entry into the RA field.
Automatic Link Local Address	Here the user can select to enable or disable the Automatic Link Local Address.

Click the **Apply** button to accept the changes made for each individual section.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the View All IPv6 Address link to view all the current IPv6 address.

Click the View All IPv6 Address link to see the following window.



Total Entries: 0

Address Type	IPv6 Address

Figure 3-13 IPv6 Interface Settings window (EI Mode Only)

Click the **<<Back** button to return to the previous page.

Management Settings

Users can stop the scrolling of multiple pages beyond the limits of the console when using the Command Line Interface.

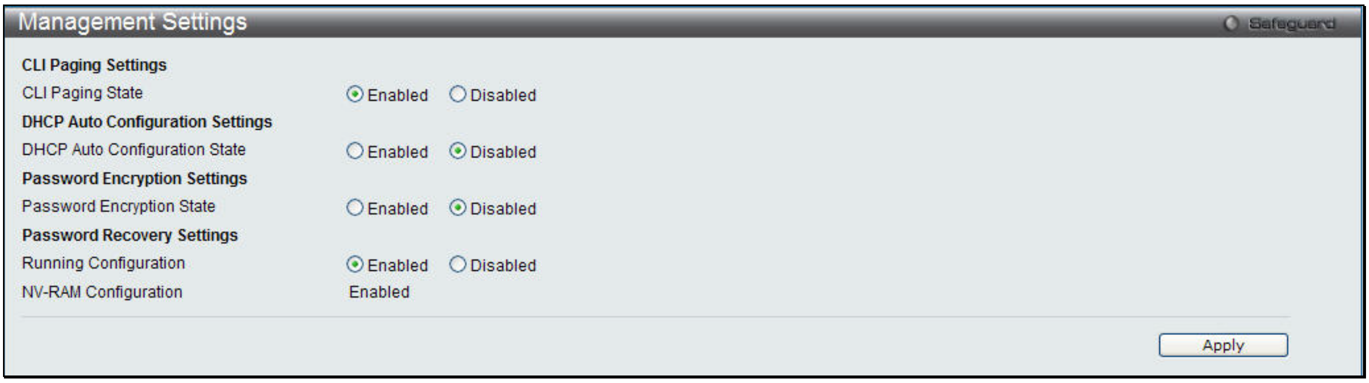
This window is also used to enable the DHCP auto configuration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the **Upload Log File** window description located in the **Tools** section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

This window also allows the user to implement the Switch's built-in power saving feature. When power saving is enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.

Users can also configure Password Encryption on the Switch.

To view the following window, click **Management > Management Settings**, as show below:



CLI Paging Settings

CLI Paging State ● Enabled ○ Disabled

DHCP Auto Configuration Settings

DHCP Auto Configuration State ○ Enabled ● Disabled

Password Encryption Settings

Password Encryption State ○ Enabled ● Disabled

Password Recovery Settings

Running Configuration ● Enabled ○ Disabled

NV-RAM Configuration Enabled

Figure 3-14 Management Settings window

The fields that can be configured are described below:

Parameter	Description
CLI Paging State	Command Line Interface paging stops each page at the end of the console. This allows you to stop the scrolling of multiple pages of text beyond the limits of the console. CLI Paging is Enabled by default. To disable it, click the Disabled radio button.

DHCP Auto Configuration State	Enable or disable the Switch's DHCP auto configuration feature. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot-up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch.
Length Detection State	Enable or disable the length detection power saving mode on the physical ports. The switch port will reduce the power feed for shorter cables.
Password Encryption State	Password encryption will encrypt the password configuration in configuration files. Password encryption is Disabled by default. To enable password encryption, click the Enabled radio button.
Running Configuration	Under the Password Recovery option, the running configuration can be enabled or disable. Being enabled, will allow the user to perform a password recovery of the running configuration.

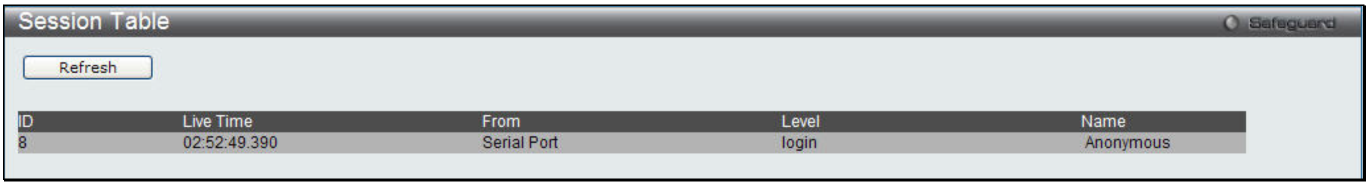
Click the **Apply** button to accept the changes made.

To learn more about the D-Link Green Technologies, go to http://green.dlink.com/ for more details.

Session Table

Users can display the management sessions since the Switch was last rebooted.

To view the following window, click **Management > Session Table**, as show below:



ID	Live Time	From	Level	Name
8	02:52:49.390	Serial Port	login	Anonymous

Figure 3-15 Session Table window

Click the **Refresh** button to refresh the display table so that new entries will appear.

Single IP Management

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the "Single IP Management" feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- A SIM group accepts up to 32 switches (numbered 1-32), not including the Commander Switch (numbered 0).

- Members of a SIM group cannot cross a router.
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain); however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The Switch may take on three different roles:

1. **Commander Switch (CS)** – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
    a. It has an IP Address.
    b. It is not a command switch or member switch of another Single IP group.
    c. It is connected to the member switches through its management VLAN.
2. **Member Switch (MS)** – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
    a. It is not a CS or MS of another IP group.
    b. It is connected to the CS through the CS management VLAN.
3. **Candidate Switch (CaS)** – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the Switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
    a. It is not a CS or MS of another Single IP group.
    b. It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Candidate state.
- CSs must change their role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.
- A MS can become a CaS by:
    - o Being configured as a CaS through the CS.
    - o If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-3120 Series switches may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, and then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

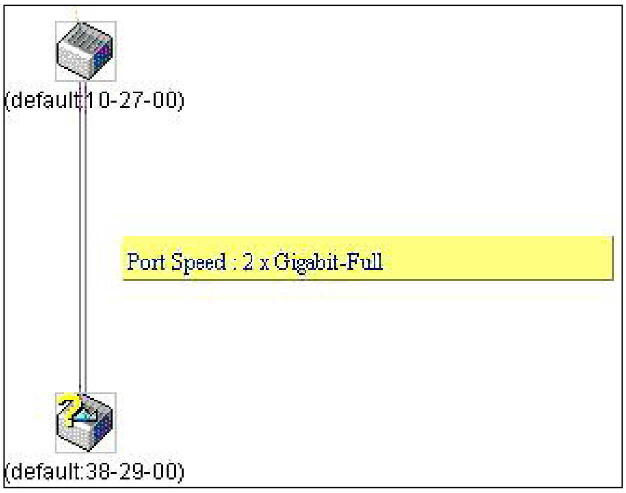
When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (includes read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

Upgrade to v1.61

To better improve SIM management, the DGS-3120 Series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintenance packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

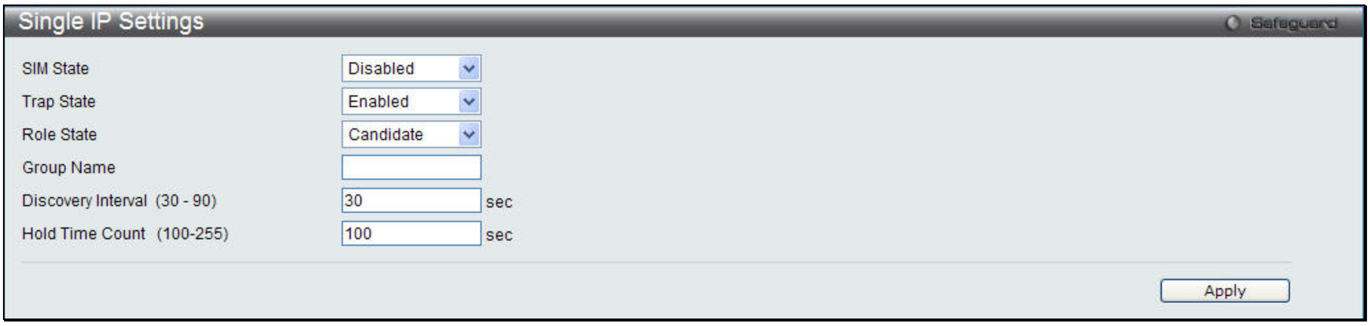


2. The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group, as shown in the adjacent picture.
3. This version will support switch upload and downloads for firmware, configuration files and log files, as follows:
   a. **Firmware** – The switch now supports MS firmware downloads from a TFTP server.
   b. **Configuration Files** – This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server.
   c. **Log** – The Switch now supports uploading MS log files to a TFTP server.
4. The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.

Single IP Settings

The Switch is set as a Candidate (CaS) as the factory default configuration and Single IP Management is disabled.

To view the following window, click **Management > Single IP Management > Single IP Settings**, as show below:



SIM State: Disabled
Trap State: Enabled
Role State: Candidate
Group Name:
Discovery Interval (30 - 90): 30 sec
Hold Time Count (100-255): 100 sec

Figure 3-16 Single IP Settings window

The fields that can be configured are described below:

Parameter	Description
SIM State	Use the drop-down menu to either enable or disable the SIM state on the Switch. *Disabled* will render all SIM functions on the Switch inoperable.
Trap State	Use the drop-down menu to enable or disable sending the trap.
Role State	Use the drop-down menu to change the SIM role of the Switch. The two choices are: *Candidate* – A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role of the Switch.

	Commander – Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter a Group Name in this textbox. This is optional. This name is used to segment switches into different SIM groups.
Discovery Interval (30-90)	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from *30* to *90* seconds. The default value is *30* seconds.
Hold Time Count (100-255)	This parameter may be set for the time, in seconds; the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from *100* to *255* seconds. The default value is *100* seconds.

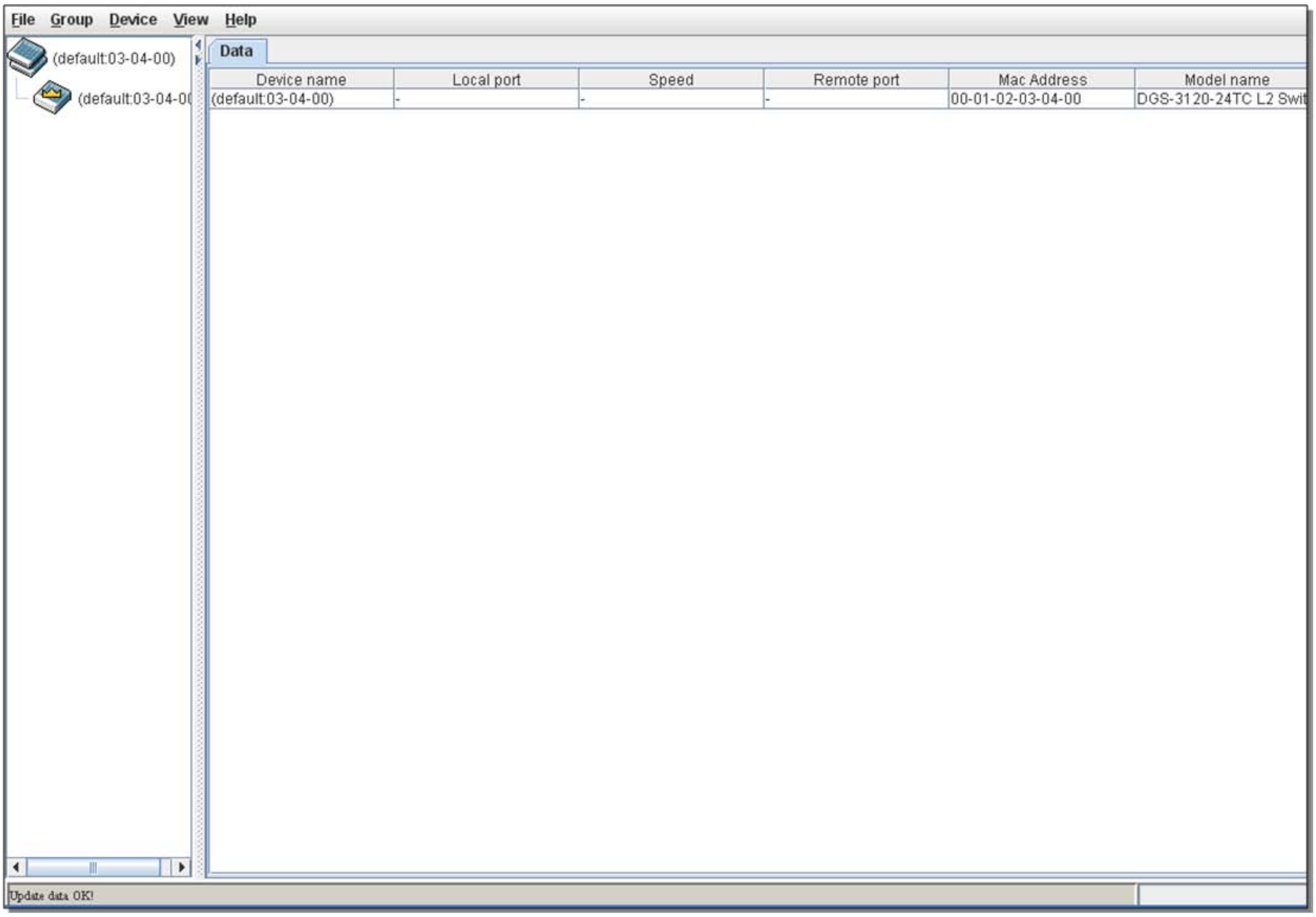
Click the **Apply** button to accept the changes made.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade**, **Configuration Backup/Restore** and **Upload Log File**.

Topology

This window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

The Java Runtime Environment on your server should initiate and lead you to the Topology window, as seen below.



Device name	Local port	Speed	Remote port	Mac Address	Model name
(default:03-04-00)	-	-	-	00-01-02-03-04-00	DGS-3120-24TC L2 Swit

Update data OK!

Figure 3-17 Single IP Management window - Tree View

The Topology window holds the following information on the **Data** tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no device is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS to which the CS is connected. The CS will have no entry in this field.
MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	Displays the full Model Name of the corresponding Switch.

To view the Topology View window, open the **View** drop-down menu in the toolbar and then click **Topology**, which will open the following Topology Map. This window will refresh itself periodically (20 seconds by default).

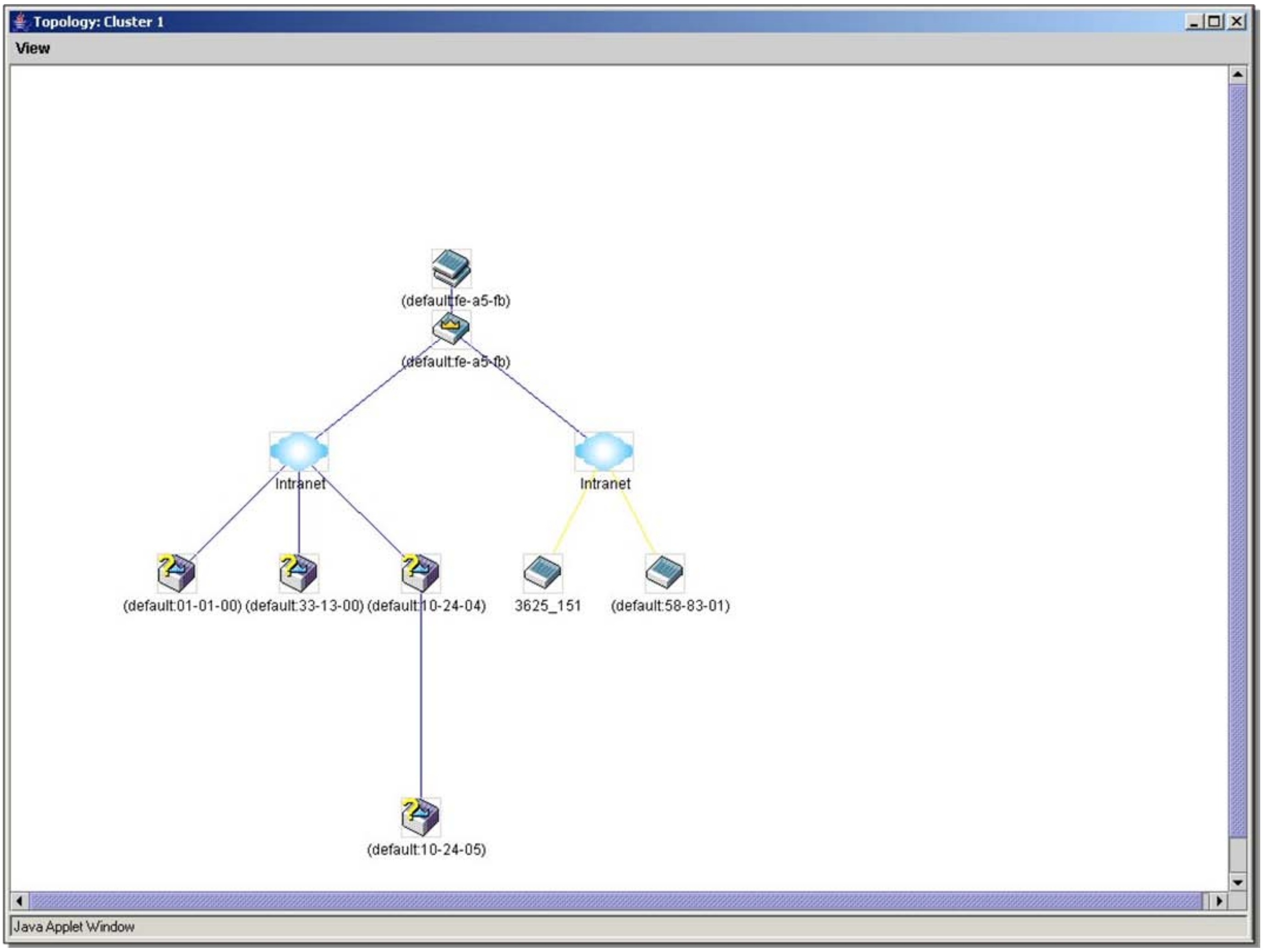

Topology: Cluster 1
View
(default:fe-a5-fb)
(default:fe-a5-fb)
Intranet
Intranet
(default:01-01-00)
(default:33-13-00)
(default:10-24-04)
3625_151
(default:58-83-01)
(default:10-24-05)
Java Applet Window

Figure 3-18 Topology view

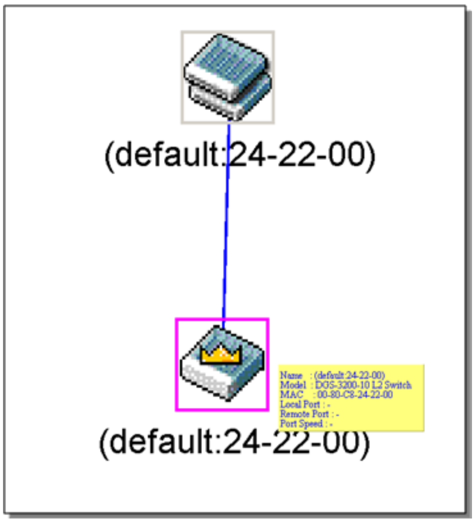
This window will display how the devices within the Single IP Management Group connect to other groups and devices. Possible icons on this window are as follows:

Icon	Description	Icon	Description

	Group		Layer 3 member switch
	Layer 2 commander switch		Member switch of other group
	Layer 3 commander switch		Layer 2 candidate switch
	Commander switch of other group		Layer 3 candidate switch
	Layer 2 member switch.		Unknown device
	Non-SIM devices		

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example.



Name : (default:24-22-00)
Model : DGS-3200-10 L2 Switch
MAC : 00-80-C8-24-22-00
Local Port : -
Remote Port : -
Port Speed : -

Figure 3-19 Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

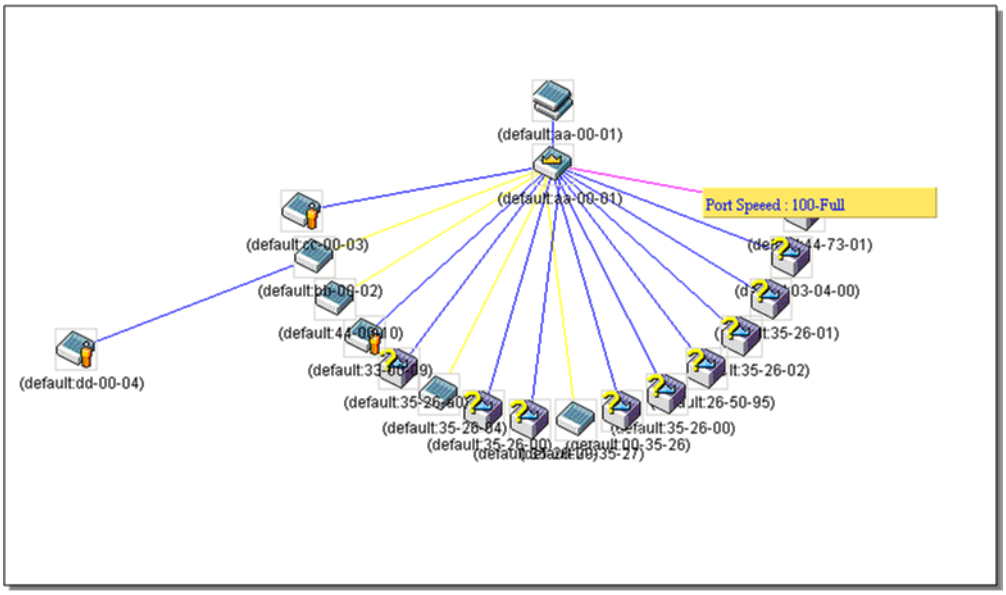

(default:aa-00-01)
(default:aa-00-01)
Port Speeed : 100-Full
(default:cc-00-03)
(default:bb-00-02)
(default:44-00-10)
(default:dd-00-04)
(default:33-00-09)
(default:35-26-a0)
(default:35-26-84)
(default:35-26-00)
(default:00-35-26)
(default:35-26-00)
(default:26-50-95)
(default:35-26-02)
(default:35-26-01)
(default:03-04-00)
(default:44-73-01)

Figure 3-20 Port Speed Utilizing the Tool Tip

Right-Click

Right-clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group Icon

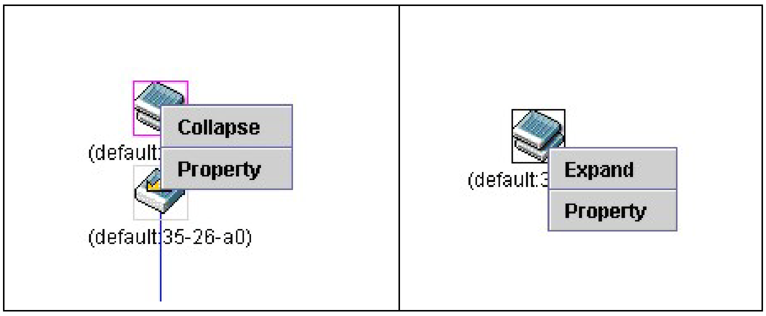
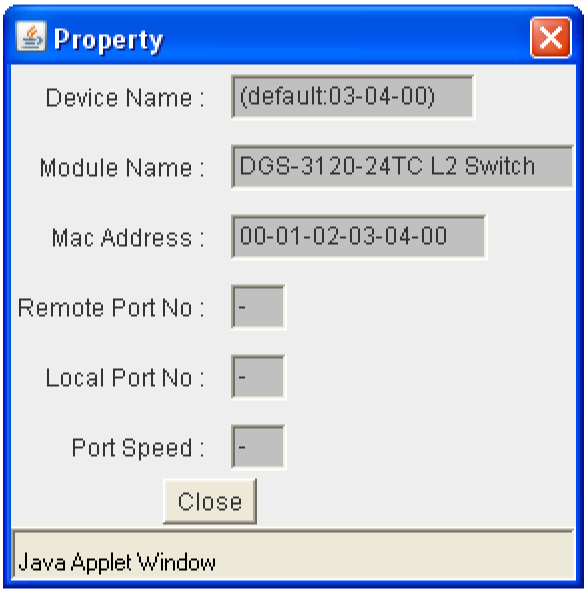

Collapse
Property
(default:
(default:35-26-a0)
(default:3
Expand
Property

Figure 3-21 Right-Clicking a Group Icon

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Property** – To pop up a window to display the group information.



Device Name : (default:03-04-00)

Module Name : DGS-3120-24TC L2 Switch

Mac Address : 00-01-02-03-04-00

Remote Port No : -

Local Port No : -

Port Speed : -

Figure 3-22 Property window

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Remote Port No	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Local Port No	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Click the **Close** button to close the property window.

Commander Switch Icon

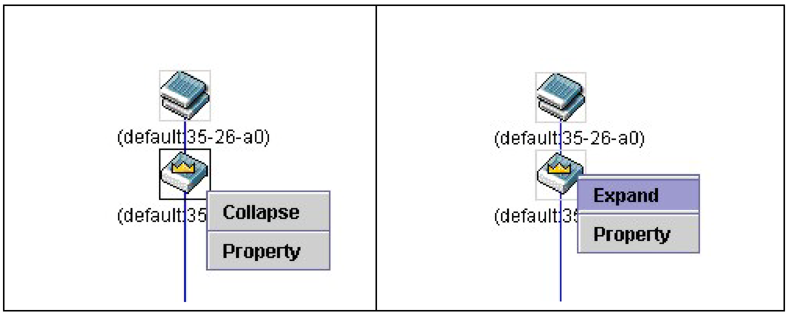


Figure 3-23 Right-clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Property** – To pop up a window to display the group information.

Member Switch Icon

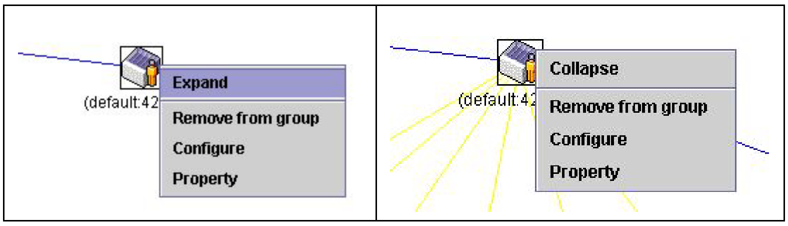

(default:42
Expand
Remove from group
Configure
Property
(default:42
Collapse
Remove from group
Configure
Property

Figure 3-24 Right-clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Remove from group** – Remove a member from a group.
- **Configure** – Launch the web management to configure the Switch.
- **Property** – To pop up a window to display the device information.

Candidate Switch Icon

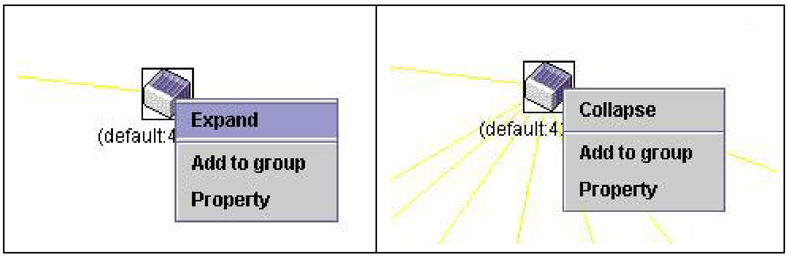

(default:4
Expand
Add to group
Property
(default:4
Collapse
Add to group
Property

Figure 3-25 Right-clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** – To collapse the group that will be represented by a single icon.
- **Expand** – To expand the SIM group, in detail.
- **Add to group** – Add a candidate to a group. Clicking this option will reveal the following dialog box for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the dialog box.

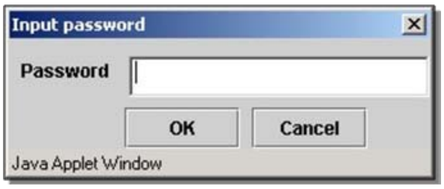

Input password
Password
OK
Cancel
Java Applet Window

Figure 3-26 Input password window

- **Property** – To pop up a window to display the device information.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.

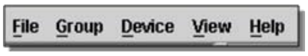

File
Group
Device
View
Help

Figure 3-27 Menu Bar of the Topology View

File

- **Print Setup** – Will view the image to be printed.
- **Print Topology** – Will print the topology map.
- **Preference** – Will set display properties, such as polling interval, and the views to open at SIM startup.

Group

- **Add to group** – Add a candidate to a group. Clicking this option will reveal the following dialog box for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the dialog box.

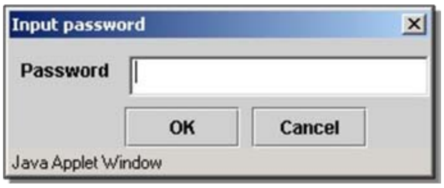


Figure 3-28 Input password window

- **Remove from Group** – Remove an MS from the group.

Device

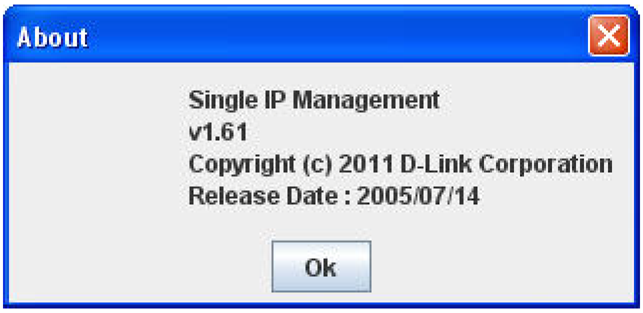
- **Configure** – Will open the Web manager for the specific device.

View

- **Refresh** – Update the views with the latest status.
- **Topology** – Display the Topology view.

Help

- **About** – Will display the SIM information, including the current SIM version.



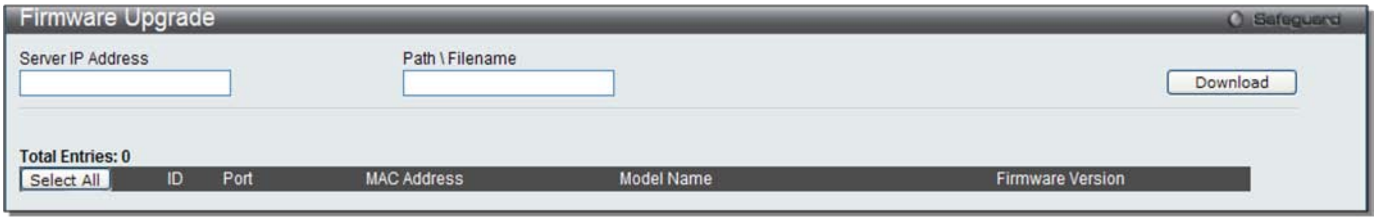
Single IP Management
v1.61
Copyright (c) 2011 D-Link Corporation
Release Date : 2005/07/14

Figure 3-29 About window

Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for firmware download, click its corresponding check box under the **Port** heading. To update the firmware, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click **Download** to initiate the file transfer.

To view the following window, click **Management > Single IP Management > Firmware Upgrade**, as show below:



Total Entries: 0

Select All	ID	Port	MAC Address	Model Name	Firmware Version

Figure 3-30 Firmware Upgrade window

Configuration File Backup/Restore

This screen is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table and will be specified by **ID**, **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Firmware Version**. To update the configuration file, enter the **Server**

IP Address where the file resides and enter the **Path/Filename** of the configuration file. Click **Restore** to initiate the file transfer from a TFTP server to the Switch. Click **Backup** to backup the configuration file to a TFTP server.

To view the following window, click **Management > Single IP Management > Configuration File Backup/Restore**, as show below:

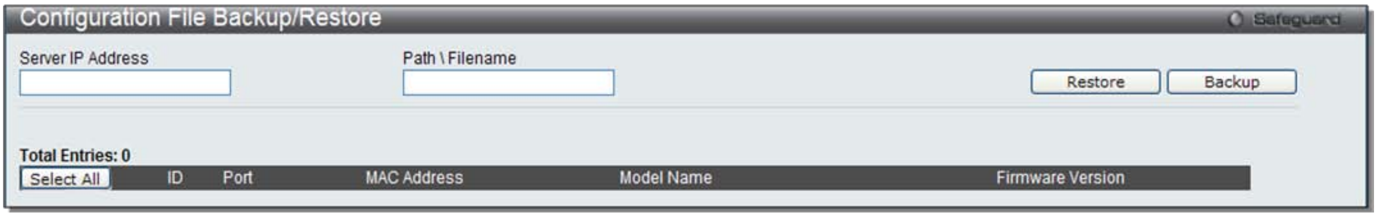


Figure 3-31 Configuration File Backup/Restore window

Upload Log File

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the Server IP address of the SIM member switch and then enter a Path\Filename on your PC where you wish to save this file. Click **Upload** to initiate the file transfer.

To view the following window, click **Management > Single IP Management > Upload Log File**, as show below:

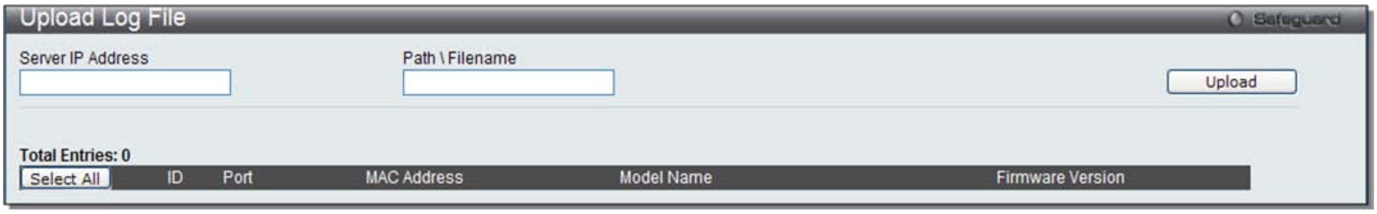


Figure 3-32 Upload Log File window

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMPv1 and SNMPv2c, user authentication is accomplished using ‘community strings’, which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMPv1 and SNMPv2c management access are:

- **public** – Allows authorized management stations to retrieve MIB objects.
- **private** – Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

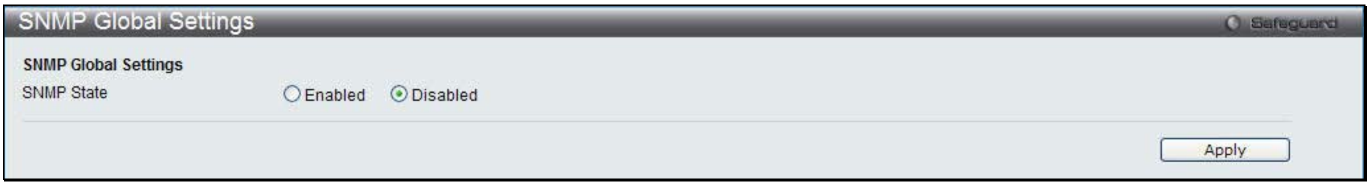
The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the Web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Global Settings

SNMP global state settings can be enabled or disabled.

To view the following window, click **Management > SNMP Settings > SNMP Global Settings**, as show below:



SNMP State ○ Enabled ● Disabled

Figure 3-33 SNMP Global Settings window

The fields that can be configured are described below:

Parameter	Description

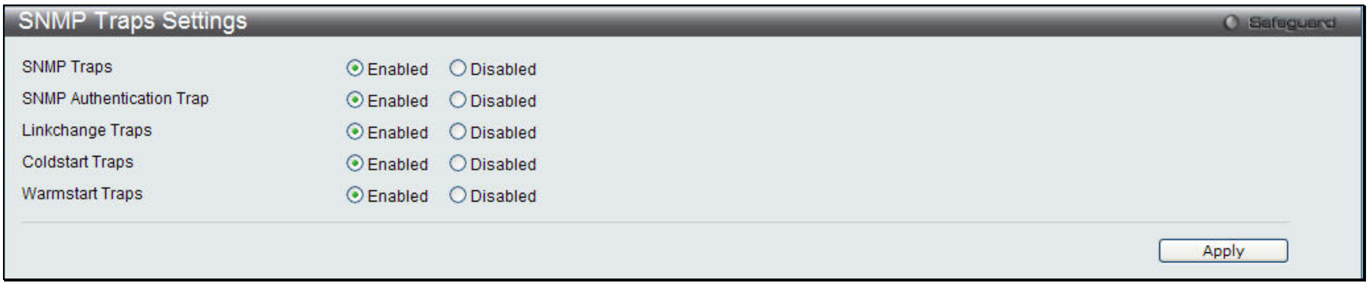
SNMP State	Enable this option to use the SNMP feature.

Click the **Apply** button to accept the changes made.

SNMP Traps Settings

Users can enable and disable the SNMP trap support function of the switch and SNMP authentication failure trap support, respectively.

To view the following window, click **Management > SNMP Settings > SNMP Traps Settings**, as show below:



SNMP Traps ● Enabled ○ Disabled
SNMP Authentication Trap ● Enabled ○ Disabled
Linkchange Traps ● Enabled ○ Disabled
Coldstart Traps ● Enabled ○ Disabled
Warmstart Traps ● Enabled ○ Disabled

Figure 3-34 SNMP Traps Settings window

The fields that can be configured are described below:

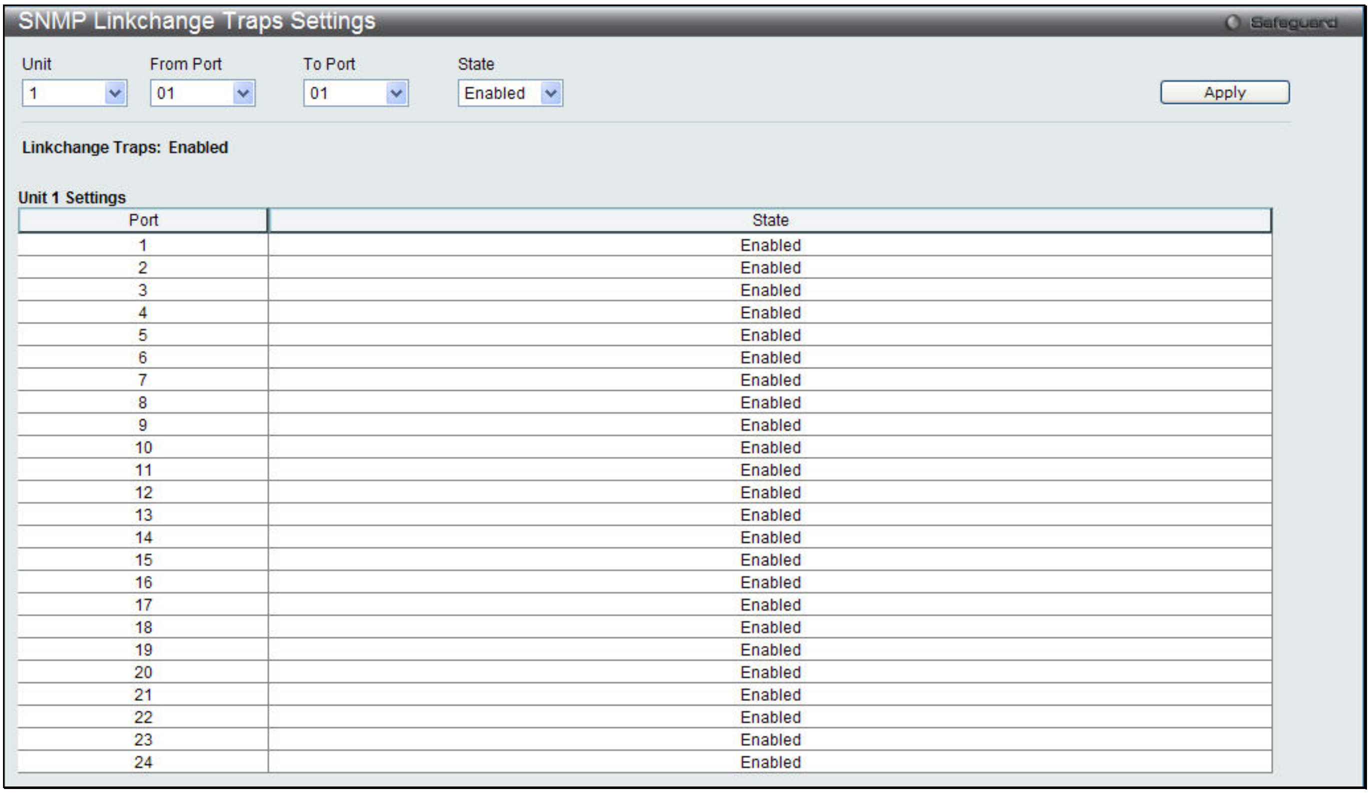
Parameter	Description
SNMP Traps	Enable this option to use the SNMP Traps feature.
SNMP Authentication Trap	Enable this option to use the SNMP Authentication Traps feature.
Linkchange Traps	Enable this option to use the SNMP Link Change Traps feature.
Coldstart Traps	Enable this option to use the SNMP Cold Start Traps feature.
Warmstart Traps	Enable this option to use the SNMP Warm Start Traps feature.

Click the **Apply** button to accept the changes made.

SNMP Linkchange Traps Settings

On this page the user can configure the SNMP link change trap settings.

To view the following window, click **Management > SNMP Settings > SNMP Linkchange Traps Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
State: Enabled

Linkchange Traps: Enabled

Unit 1 Settings

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled
11	Enabled
12	Enabled
13	Enabled
14	Enabled
15	Enabled
16	Enabled
17	Enabled
18	Enabled
19	Enabled
20	Enabled
21	Enabled
22	Enabled
23	Enabled
24	Enabled

Figure 3-35 SNMP Linkchange Traps Settings window

The fields that can be configured are described below:

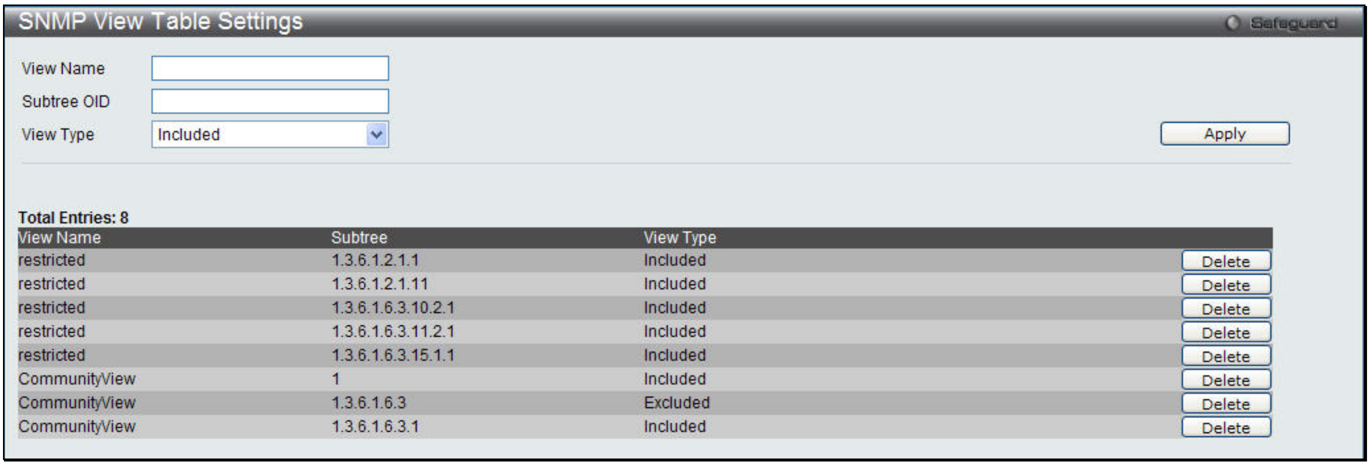
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the starting and ending ports to use.
State	Use the drop-down menu to enable or disable the SNMP link change Trap.

Click the **Apply** button to accept the changes made.

SNMP View Table Settings

Users can assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

To view the following window, click **Management > SNMP Settings > SNMP View Table Settings**, as show below:



View Name:
Subtree OID:
View Type: Included

Total Entries: 8

View Name	Subtree	View Type	
restricted	1.3.6.1.2.1.1	Included	Delete
restricted	1.3.6.1.2.1.11	Included	Delete
restricted	1.3.6.1.6.3.10.2.1	Included	Delete
restricted	1.3.6.1.6.3.11.2.1	Included	Delete
restricted	1.3.6.1.6.3.15.1.1	Included	Delete
CommunityView	1	Included	Delete
CommunityView	1.3.6.1.6.3	Excluded	Delete
CommunityView	1.3.6.1.6.3.1	Included	Delete

Figure 3-36 SNMP View Table Settings window

The fields that can be configured are described below:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

Click the **Apply** button to accept the changes made.

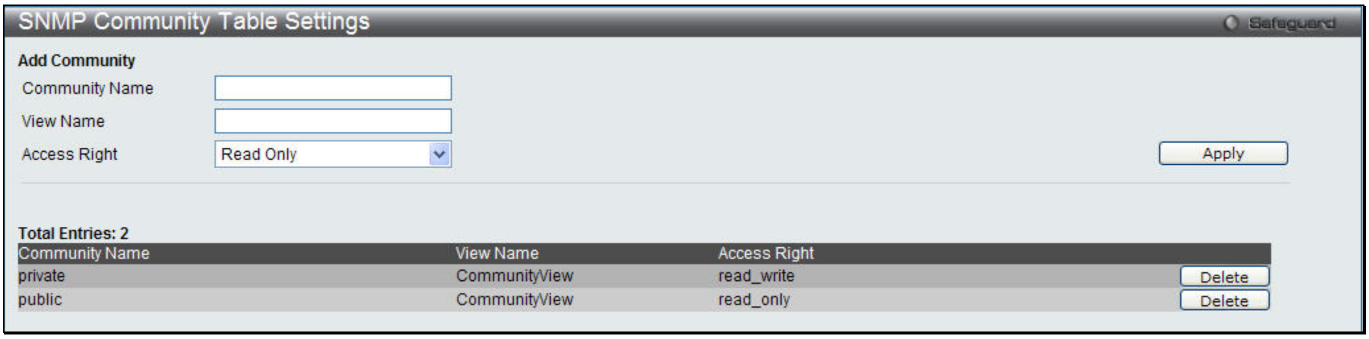
Click the **Delete** button to remove the specific entry.

SNMP Community Table Settings

Users can create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To view the following window, click **Management > SNMP Settings > SNMP Community Table Settings**, as show below:



Community Name
View Name
Access Right: Read Only

Total Entries: 2

Community Name	View Name	Access Right
private	CommunityView	read_write
public	CommunityView	read_only

Figure 3-37 SNMP Community Table Settings window

The fields that can be configured are described below:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	*Read Only* – Specify that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* – Specify that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

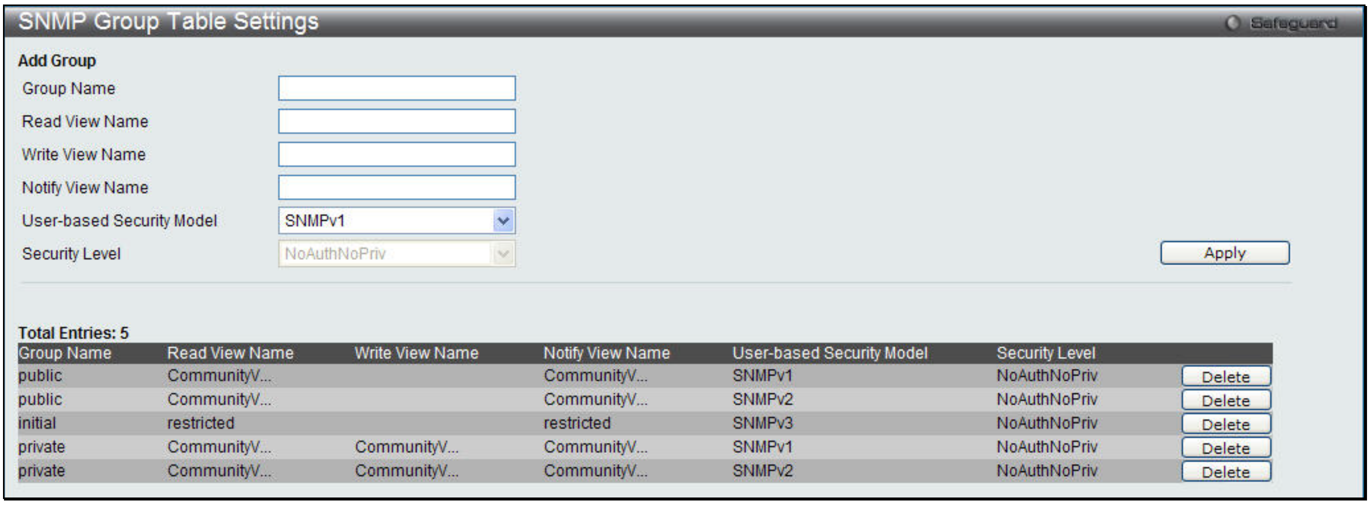
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

SNMP Group Table Settings

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

To view the following window, click **Management > SNMP Settings > SNMP Group Table Settings**, as show below:



Add Group

Group Name

Read View Name

Write View Name

Notify View Name

User-based Security Model: SNMPv1

Security Level: NoAuthNoPriv

Total Entries: 5

Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level	
public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	Delete
public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	Delete
initial	restricted		restricted	SNMPv3	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv	Delete

Figure 3-38 SNMP Group Table Settings window

The fields that can be configured are described below:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
User-based Security Model	*SNMPv1* – Specify that SNMP version 1 will be used. *SNMPv2* – Specify that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *SNMPv3* – Specify that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.
Security Level	The Security Level settings only apply to SNMPv3. *NoAuthNoPriv* – Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *AuthNoPriv* – Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *AuthPriv* – Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

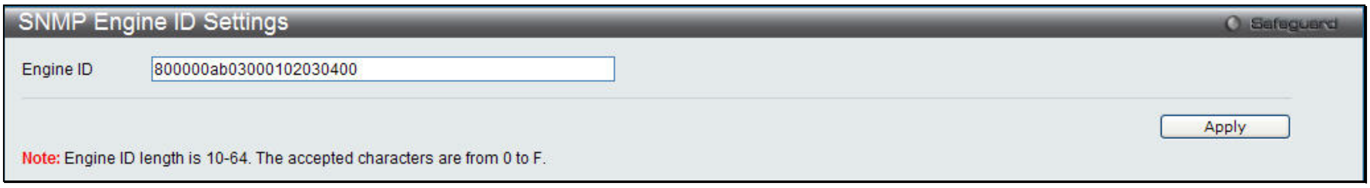
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

SNMP Engine ID Settings

The Engine ID is a unique identifier used for SNMP V3 implementations on the Switch.

To view the following window, click **Management > SNMP Settings > SNMP Engine ID Settings**, as show below:



Engine ID: 800000ab03000102030400

Note: Engine ID length is 10-64. The accepted characters are from 0 to F.

Figure 3-39 SNMP Engine ID Settings window

The fields that can be configured are described below:

Parameter	Description
Engine ID	To change the Engine ID, type the new Engine ID value in the space provided. The SNMP engine ID displays the identification of the SNMP engine on the Switch. The default value is suggested in RFC2271. The very first bit is 1, and the first four octets are set to the binary equivalent of the agent's SNMP management private enterprise number as assigned by IANA (D-Link is 171). The fifth octet is 03 to indicate the rest is the MAC address of this device. The sixth to eleventh octets is the MAC address.

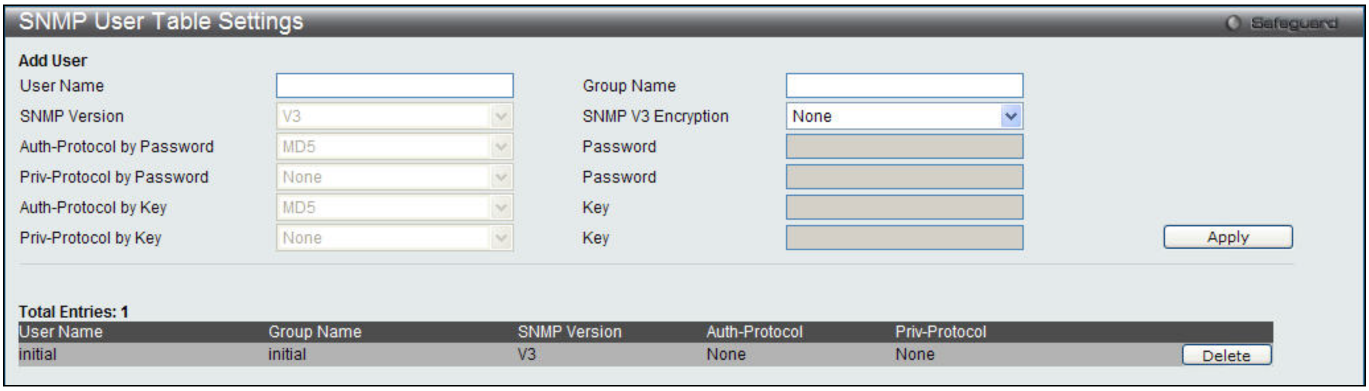
Click the **Apply** button to accept the changes made.

NOTE: The Engine ID length is 10-64 and accepted characters can range from 0 to F.

SNMP User Table Settings

This window displays all of the SNMP User's currently configured on the Switch.

To view the following window, click **Management > SNMP Settings > SNMP User Table Settings**, as show below:



User Name		Group Name	
SNMP Version	V3	SNMP V3 Encryption	None
Auth-Protocol by Password	MD5	Password	
Priv-Protocol by Password	None	Password	
Auth-Protocol by Key	MD5	Key	
Priv-Protocol by Key	None	Key	

Total Entries: 1

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol
initial	initial	V3	None	None

Figure 3-40 SNMP User Table Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	*V3* – Indicates that SNMP version 3 is in use.
SNMP V3 Encryption	Use the drop-down menu to enable encryption for SNMP V3. This is only operable in SNMP V3 mode. The choices are *None*, *Password*, or *Key*.

Auth-Protocol	*MD5* – Specify that the HMAC-MD5-96 authentication level will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password. *SHA* – Specify that the HMAC-SHA authentication protocol will be used. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.
Priv-Protocol	*None* – Specify that no authorization protocol is in use. *DES* – Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when *V3* is selected in the SNMP Version field and the Encryption field has been checked. This field will require the user to enter a password.

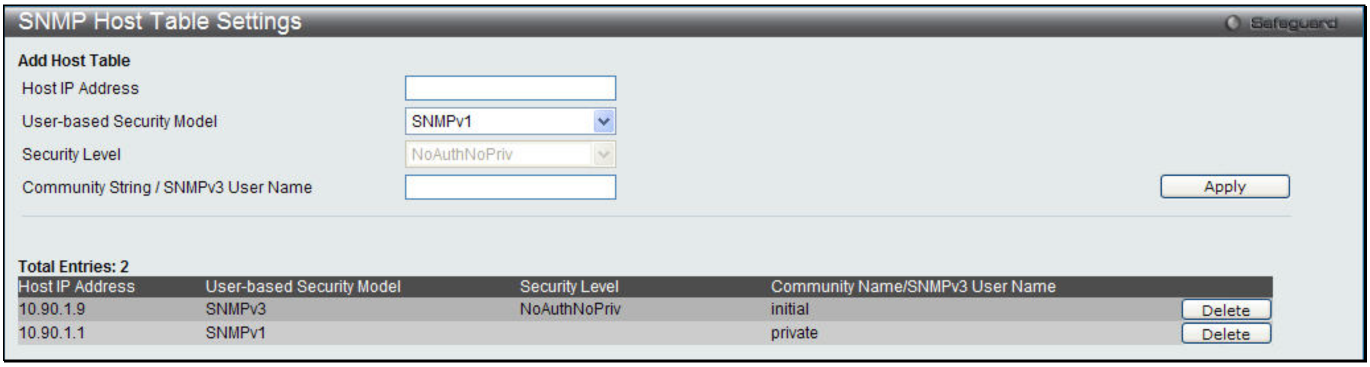
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

SNMP Host Table Settings

Users can set up SNMP trap recipients for IPv4.

To view the following window, click **Management > SNMP Settings > SNMP Host Table Settings**, as show below:



SNMP Host Table Settings

Add Host Table

Host IP Address:

User-based Security Model: SNMPv1

Security Level: NoAuthNoPriv

Community String / SNMPv3 User Name:

Total Entries: 2

Host IP Address	User-based Security Model	Security Level	Community Name/SNMPv3 User Name	
10.90.1.9	SNMPv3	NoAuthNoPriv	initial	Delete
10.90.1.1	SNMPv1		private	Delete

Figure 3-41 SNMP Host Table Settings window

The fields that can be configured are described below:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* – Specify that SNMP version 1 will be used. *SNMPv2* – Specify that SNMP version 2 will be used. *SNMPv3* – Specify that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. *AuthNoPriv* – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. *AuthPriv* – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMPv3 User Name	Type in the community string or SNMP V3 user name as appropriate.

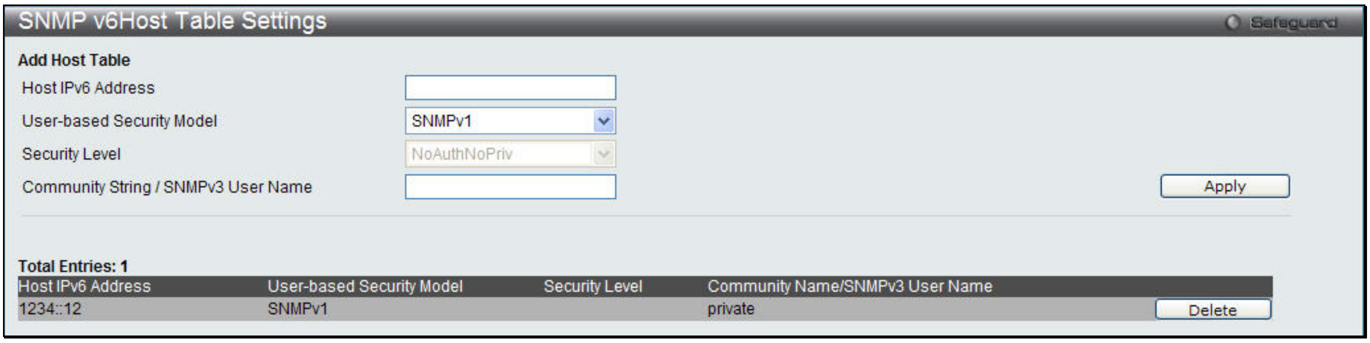
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

SNMPv6 Host Table Settings (EI Mode Only)

Users can set up SNMP trap recipients for IPv6.

To view the following window, click **Management > SNMP Settings > SNMPv6 Host Table Settings**, as show below:



Add Host Table

Host IPv6 Address

User-based Security Model: SNMPv1

Security Level: NoAuthNoPriv

Community String / SNMPv3 User Name

Total Entries: 1

Host IPv6 Address	User-based Security Model	Security Level	Community Name/SNMPv3 User Name
1234::12	SNMPv1		private

3-42 SNMPv6 Host Table Settings

The fields that can be configured are described below:

Parameter	Description
Host IPv6 Address	Type the IPv6 address of the remote management station that will serve as the SNMP host for the Switch.
User-based Security Model	*SNMPv1* – Specifies that SNMP version 1 will be used. *SNMPv2* – Specifies that SNMP version 2 will be used. *SNMPv3* – Specifies that SNMP version 3 will be used.
Security Level	*NoAuthNoPriv* – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level. *AuthNoPriv* – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level. *AuthPriv* – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.
Community String / SNMPv3 User Name	Type in the community string or SNMP V3 user name as appropriate.

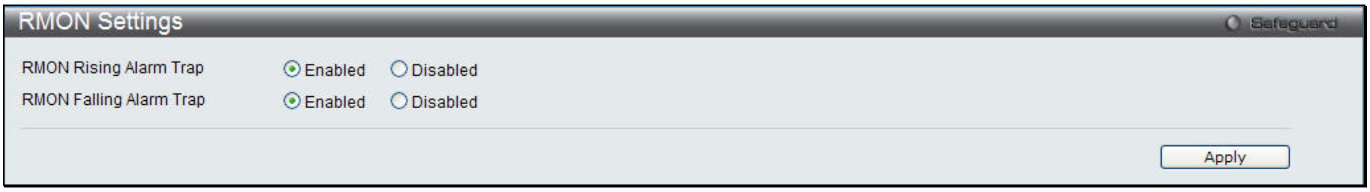
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

RMON Settings

On this page the user can enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.

To view the following window, click **Management > SNMP Settings > RMON Settings**, as show below:



RMON Rising Alarm Trap ● Enabled ○ Disabled

RMON Falling Alarm Trap ● Enabled ○ Disabled

Figure 3-43 RMON Settings window

The fields that can be configured are described below:

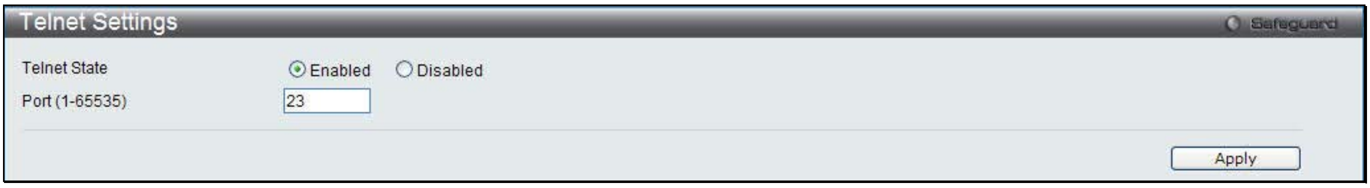
Parameter	Description
RMON Rising Alarm Trap	Enable this option to use the RMON Rising Alarm Trap Feature.
RMON Falling Alarm Trap	Enable this option to use the RMON Falling Alarm Trap Feature.

Click the **Apply** button to accept the changes made.

Telnet Settings

Users can configure Telnet Settings on the Switch.

To view the following window, click **Management > Telnet Settings**, as show below:



Telnet State ● Enabled ○ Disabled

Port (1-65535) 23

Figure 3-44 Telnet Settings window

The fields that can be configured are described below:

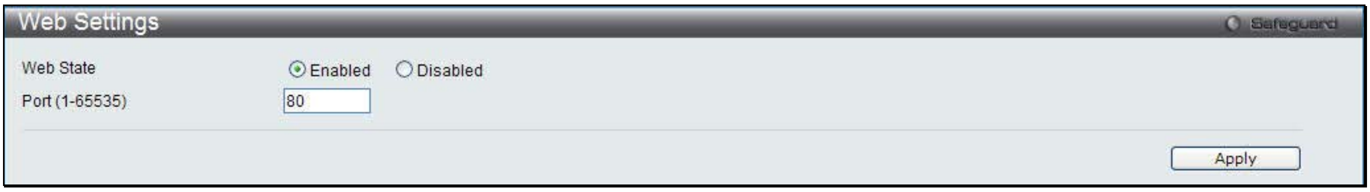
Parameter	Description
Telnet State	Telnet configuration is Enabled by default. If you do not want to allow configuration of the system through Telnet choose Disabled.
Port (1-65535)	The TCP port number used for Telnet management of the Switch. The “well-known” TCP port for the Telnet protocol is *23*.

Click the **Apply** button to accept the changes made.

Web Settings

Users can configure the Web settings on the Switch.

To view the following window, click **Management > Web Settings**, as show below:



Web State ● Enabled ○ Disabled

Port (1-65535) 80

Figure 3-45 Web Settings window

The fields that can be configured are described below:

Parameter	Description
Web Status	Web-based management is Enabled by default. If you choose to disable this by clicking Disabled, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
Port (1-65535)	The TCP port number used for web-based management of the Switch. The “well-known” TCP port for the Web protocol is *80*.

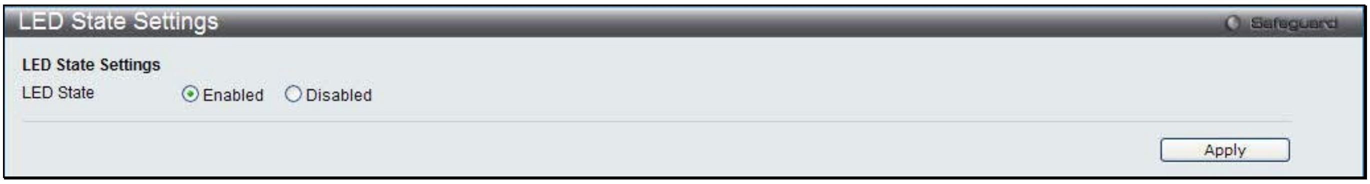
Click the **Apply** button to accept the changes made.

Power Saving

LED State Settings

This window is used to configure the port LED state.

To view the following window, click **Management > Power Saving > LED State Settings**, as show below:



LED State Settings

LED State ● Enabled ○ Disabled

Figure 3-46 LED State Settings window

The fields that can be configured are described below:

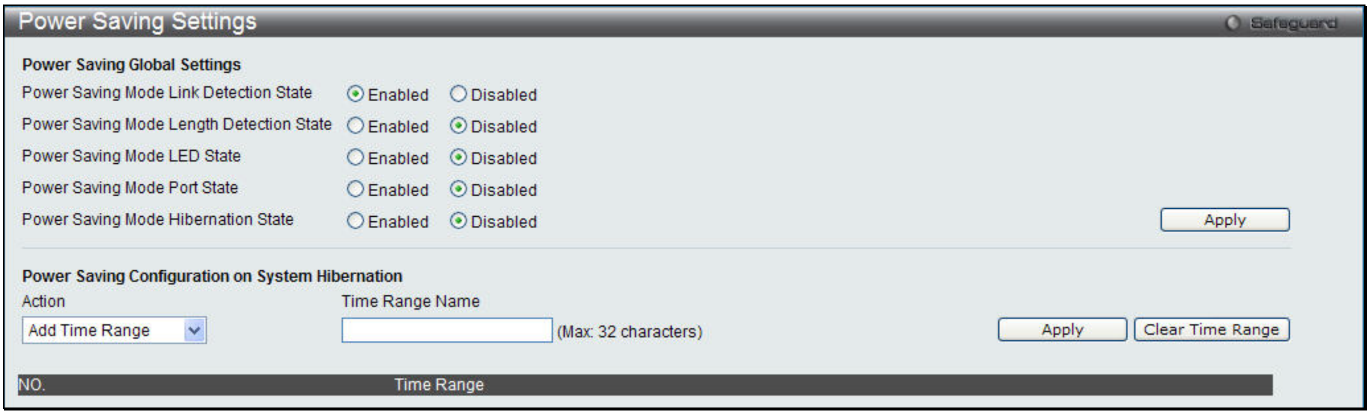
Parameter	Description
LED State	Click the radio buttons to enable or disable the port LED state.

Click the **Apply** button to accept the changes made.

Power Saving Settings

This window allows the user to implement the Switch's built-in power saving features and set the schedule to enforce the settings.

To view the following window, click **Management > Power Saving > Power Saving Settings**, as show below:



Power Saving Global Settings

Power Saving Mode Link Detection State ● Enabled ○ Disabled

Power Saving Mode Length Detection State ○ Enabled ● Disabled

Power Saving Mode LED State ○ Enabled ● Disabled

Power Saving Mode Port State ○ Enabled ● Disabled

Power Saving Mode Hibernation State ○ Enabled ● Disabled

Power Saving Configuration on System Hibernation

Action: Add Time Range

Time Range Name: (Max: 32 characters)

Figure 3-47 Power Saving Settings window

The fields that can be configured are described below:

Parameter	Description
Power Saving Mode Link Detection State	Click the radio buttons to enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.
Power Saving Mode Length Detection State	Click the radio buttons to enable or disable length detection state. When enabled, the Switch will automatically determine the length of the cable and adjust the power flow accordingly.
Power Saving Mode LED State	Click the radio buttons to enable or disable LED state. When enabled, the LED's state of ports will be turned off during the configured time range.
Power Saving Mode	Click the radio buttons to enable or disable port state. When enabled, the ports will

Port State	be shut down during the configured time range.
Power Saving Mode Hibernation State	Click the radio buttons to enable or disable hibernation state. When enabled, the Switch will go into a low power state and be idle during the configured time range. It will shut down all the ports, all network function (telnet, ping, etc.) will not work, and only the console connection will work via the RS232 port. If the Switch is an endpoint type PSE (Power Sourcing Equipment), it will not provide power to the port.
Action	Use the drop down menu to add or delete the schedule.
Time Range Name	Specify the name of the schedule.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear Time Range** to remove all the entries.

Power Saving LED Settings

This window is used to add or delete the power saving schedule on the LED of all ports.

To view the following window, click **Management > Power Saving > Power Saving LED Settings**, as show below:

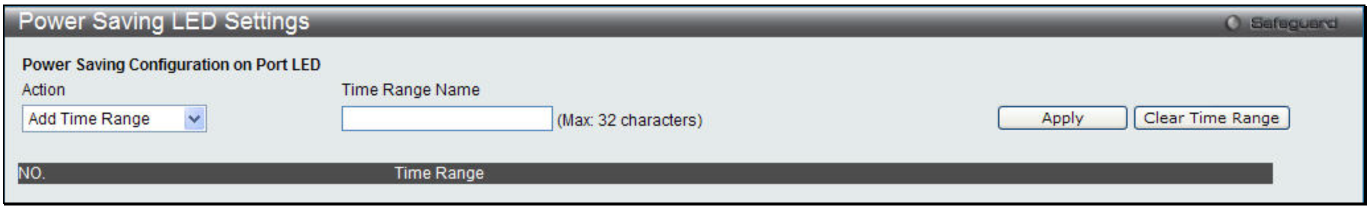

Power Saving LED Settings
Safeguard
Power Saving Configuration on Port LED
Action
Time Range Name
Add Time Range
(Max: 32 characters)
Apply
Clear Time Range
NO.
Time Range

Figure 3-48 Power Saving LED Settings window

The fields that can be configured are described below:

Parameter	Description
Action	Use the drop down menu to add or delete the schedule.
Time Range Name	Specify the name of the schedule.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear Time Range** to remove all the entries.

Power Saving Port Settings

This window is used to set the power saving state.

To view the following window, click **Management > Power Saving > Power Saving Port Settings**, as show below:

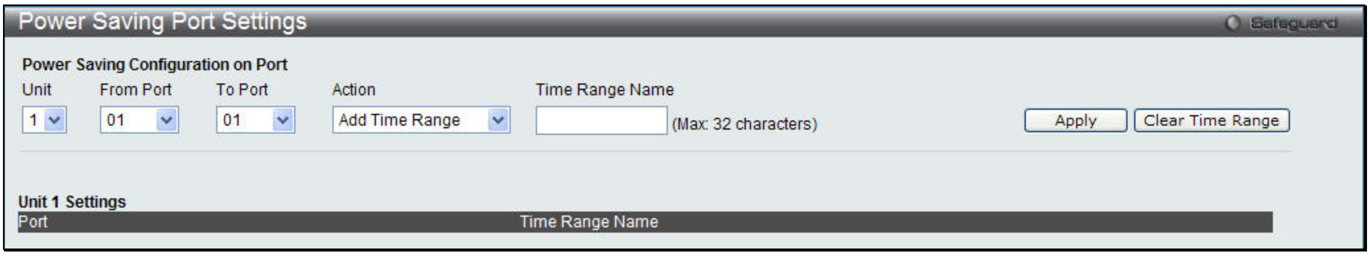

Power Saving Port Settings
Safeguard
Power Saving Configuration on Port
Unit
From Port
To Port
Action
Time Range Name
1
01
01
Add Time Range
(Max: 32 characters)
Apply
Clear Time Range
Unit 1 Settings
Port
Time Range Name

Figure 3-49 Power Saving Port Settings

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Select the appropriate port range used for the configuration.

Action	Use the drop down menu to add or delete the schedule.
Time Range Name	Specify the name of the schedule.

Click the **Apply** button to accept the changes made for each individual section.

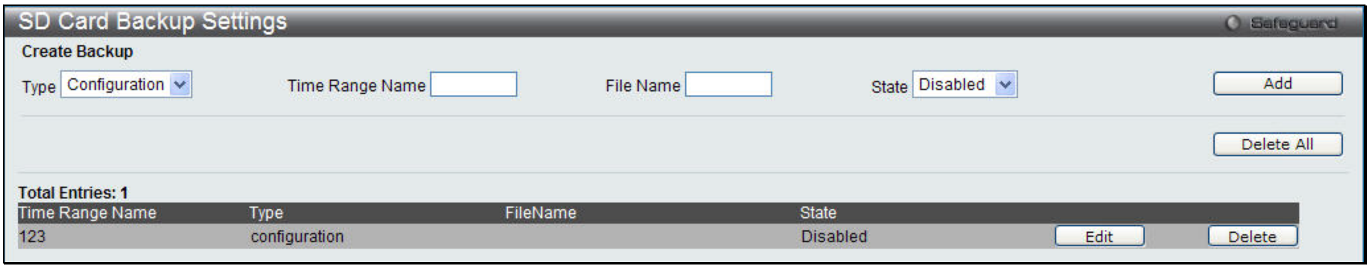
Click the **Clear Time Range** to remove all the entries.

SD Card Management

SD Card Backup Settings

This window is used to create a schedule to back up the configuration or log to file system.

To view the following window, click **Management > SD Card Management > SD Card Backup Settings**, as show below:



Type: Configuration
Time Range Name:
File Name:
State: Disabled

Total Entries: 1

Time Range Name	Type	FileName	State		
123	configuration		Disabled	Edit	Delete

Figure 3-50 SD Card Backup Settings window

The fields that can be configured are described below:

Parameter	Description
Type	Use the drop-down menu to back up configuration or log.
Time Range Name	Specify the schedule to back up the configuration or log.
File Name	Specify the backup file name.
State	Use the drop-down menu to enable or disable the backup schedule.

Click **Add** to create a new entry.

Click **Delete All** to remove all the entries from the table.

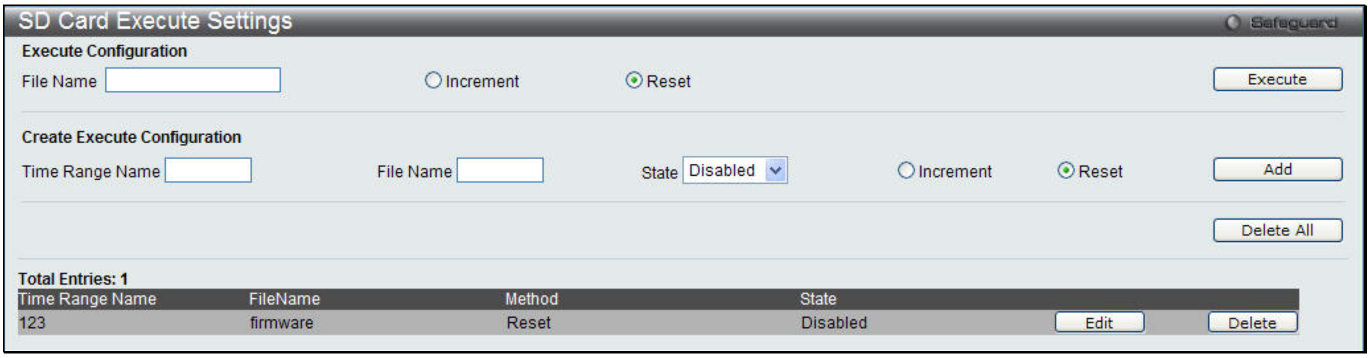
Click **Edit** to modify the specific entry.

Click **Delete** to remove the specific entry.

SD Card Execute Settings

This window is used to configure a schedule to execute the configuration on file system.

To view the following window, click **Management > SD Card Management > SD Card Execute Settings**, as show below:



Execute Configuration

File Name ☐ ○ Increment ● Reset

Create Execute Configuration

Time Range Name ☐ File Name ☐ State Disabled ○ Increment ● Reset

Total Entries: 1

Time Range Name	FileName	Method	State
123	firmware	Reset	Disabled

Figure 3-51 SD Card Execute Settings window

The fields that can be configured are described below:

Parameter	Description
File Name	The filename of the configuration on file system.
Increment	If this option is specified, the current configuration will not be reset before executing the configuration.
Reset	If this option is specified, the current configuration will be reset before executing the configuration.
Time Range Name	The time range for schedule to execute the configuration.
State	Enable or disable the executive schedules.

Click **Execute** to execute configuration on file system.

Click **Add** to create a new entry.

Click **Delete All** to remove all the entries from the table.

Click **Edit** to modify the specific entry.

Click **Delete** to remove the specific entry.

Chapter 4 L2 Features

VLAN
QinQ (EI Mode Only)
Layer 2 Protocol Tunneling Settings
Spanning Tree
Link Aggregation
FDB
L2 Multicast Control
Multicast Filtering
ERPS Settings (EI Mode Only)
LLDP
NLB FDB Settings

VLAN

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the Switch

- No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.
- The Switch supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.
- The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."
- The "default" VLAN has a VID = 1.
- The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.
- **Ingress port** – A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.
- **Egress port** – A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
  - Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
  - Forwarding rules between ports – decides whether to filter or forward the packet.
  - Egress rules – determines if the packet must be sent tagged or untagged.

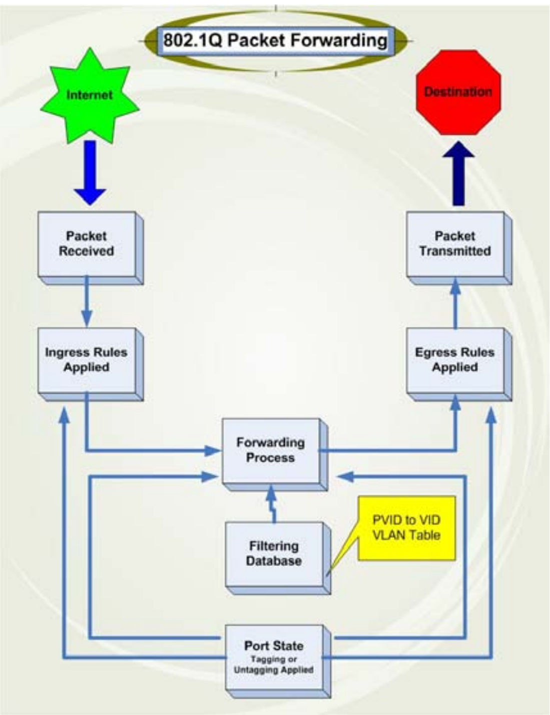

802.1Q Packet Forwarding
Internet
Destination
Packet Received
Packet Transmitted
Ingress Rules Applied
Egress Rules Applied
Forwarding Process
PVID to VID VLAN Table
Filtering Database
Port State
Tagging or Untagging Applied

Figure 4-1 IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

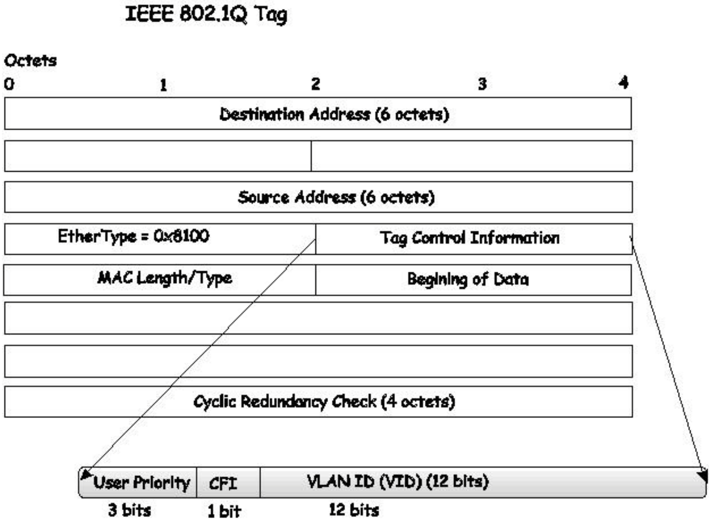

IEEE 802.1Q Tag
Octets
0
1
2
3
4
Destination Address (6 octets)
Source Address (6 octets)
EtherType = 0x8100
Tag Control Information
MAC Length/Type
Begining of Data
Cyclic Redundancy Check (4 octets)
User Priority
CFI
VLAN ID (VID) (12 bits)
3 bits
1 bit
12 bits

Figure 4-2 IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

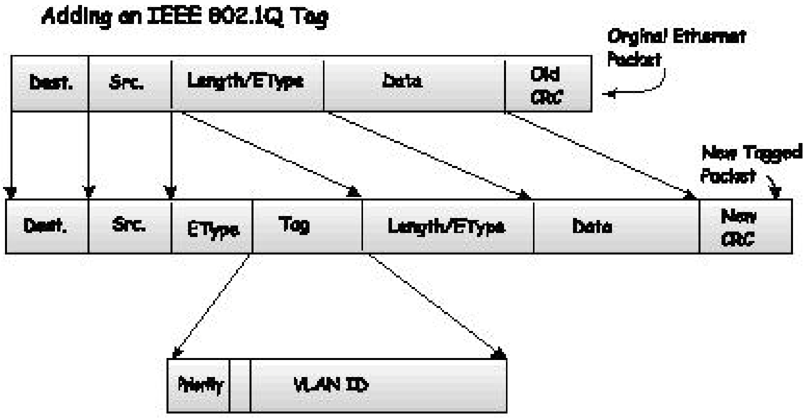


Figure 4-3 Adding an IEEE 802.1Q Tag

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it.

If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7
Engineering	2	9, 10
Sales	5	1, 2, 3, 4

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

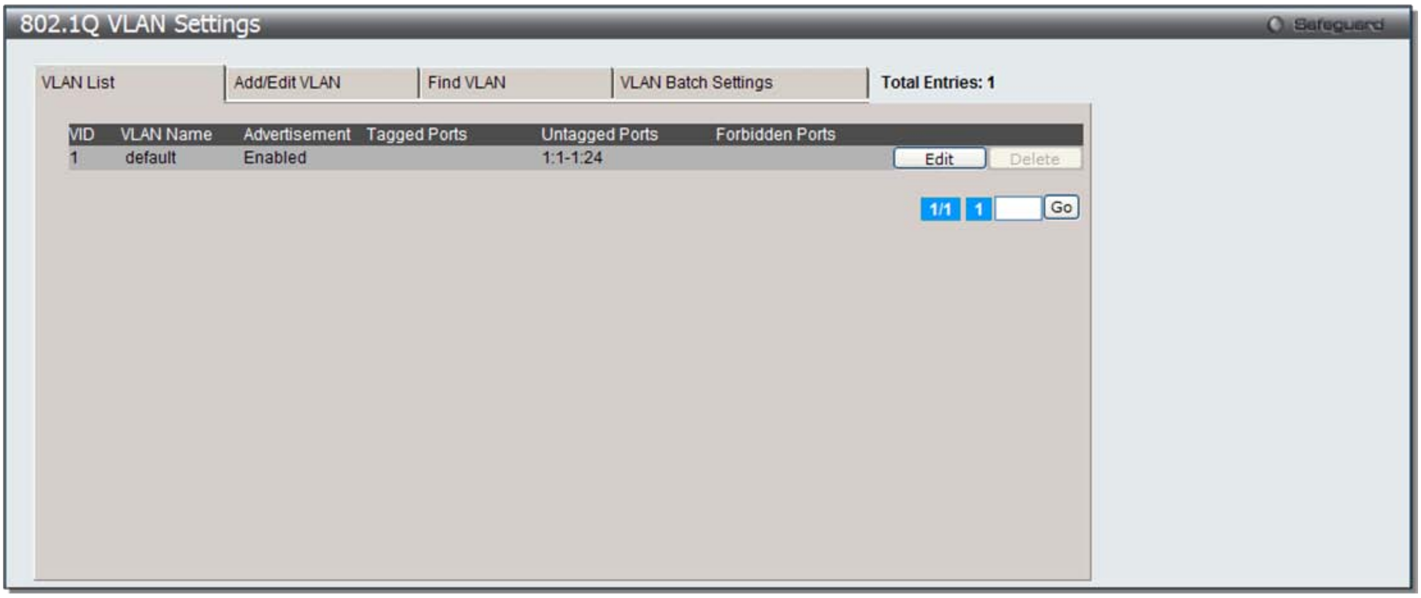
VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

802.1Q VLAN Settings

The **VLAN List** tab lists all previously configured VLANs by VLAN ID and VLAN Name.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN Settings**, as show below:



Total Entries: 1

VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports	
1	default	Enabled		1:1-1:24		Edit Delete

Figure 4-4 802.1Q VLAN Settings –VLAN List Tab window

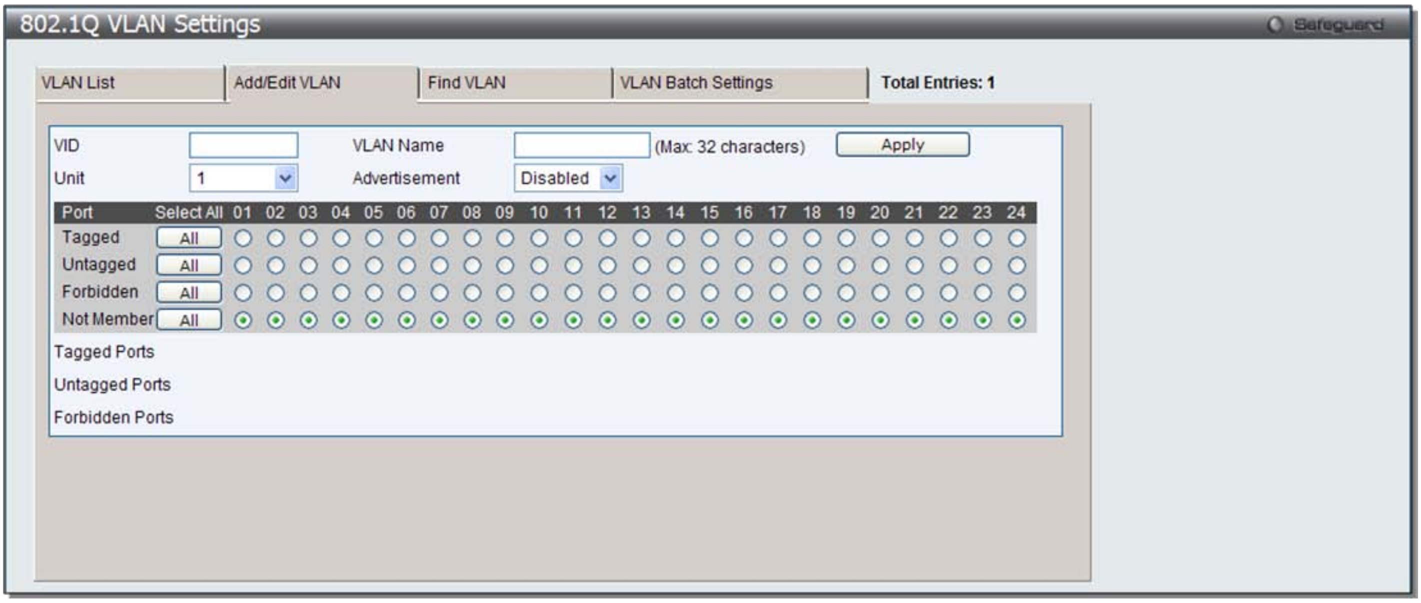
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

To create a new 802.1Q VLAN or modify an existing 802.1Q VLAN, click the **Add/Edit VLAN** tab.

A new tab will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN.



Total Entries: 1

VID

VLAN Name (Max: 32 characters)

Unit: 1

Advertisement: Disabled

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Untagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Figure 4-5 802.1Q VLAN Settings – Add/Edit VLAN Tab window

The fields that can be configured are described below:

Parameter	Description
VID	Allow the entry of a VLAN ID or displays the VLAN ID of an existing VLAN in the **Add/Edit VLAN** tab. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allow the entry of a name for the new VLAN or for editing the VLAN name in the **Add/Edit VLAN** tab.
Advertisement	Enable this function to allow the Switch sending out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Unit	Select the unit you want to configure.
Port	Display all ports of the Switch for the configuration option.
Tagged	Specify the port as 802.1Q tagging. Clicking the radio button will designate the port as tagged. Click the **All** button to select all ports.
Untagged	Specify the port as 802.1Q untagged. Clicking the radio button will designate the port as untagged. Click the **All** button to select all ports.
Forbidden	Click the radio button to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically. Click the **All** button to select all ports.
Not Member	Click the radio button to allow an individual port to be specified as a non-VLAN member. Click the **All** button to select all ports.

Click the **Apply** button to accept the changes made.

To search for a VLAN, click the **Find VLAN** tab. A new tab will appear, as shown below.

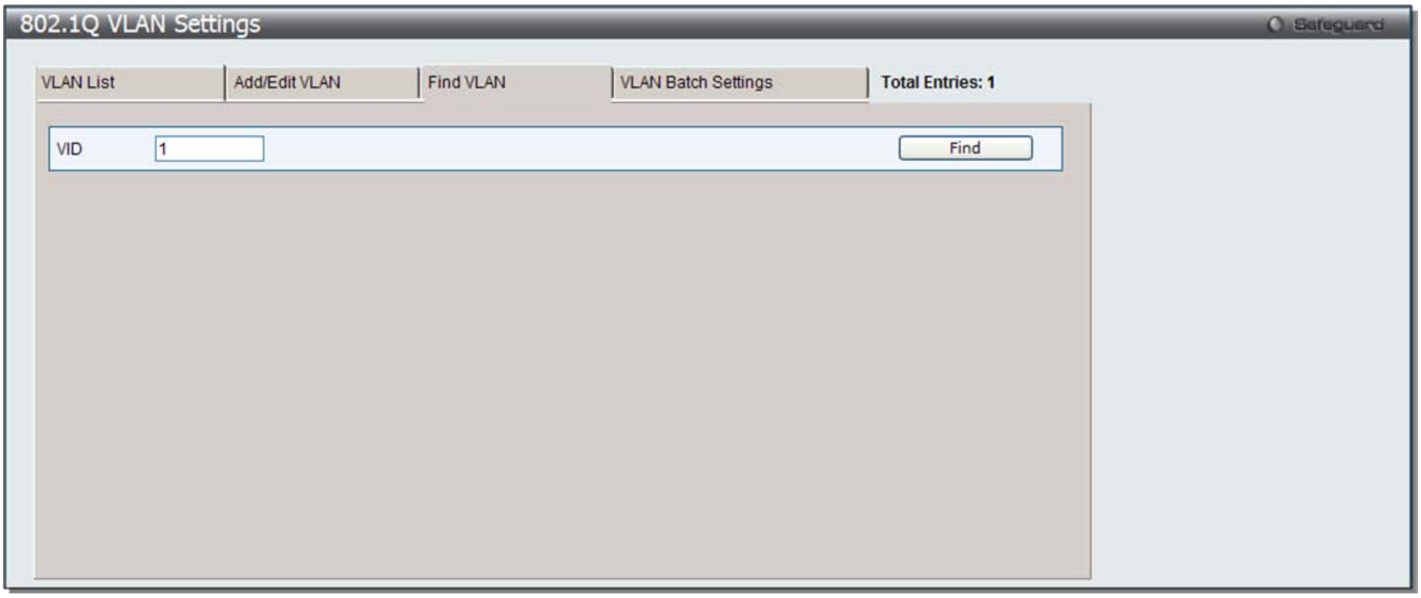

802.1Q VLAN Settings
Safeguard
VLAN List
Add/Edit VLAN
Find VLAN
VLAN Batch Settings
Total Entries: 1
VID
1
Find

Figure 4-6 802.1Q VLAN Settings – Find VLAN Tab window

Enter the VLAN ID number in the field offered and then click the **Find** button. You will be redirected to the **VLAN List** tab.

To create, delete and configure a VLAN Batch entry click the **VLAN Batch Settings** tab, as shown below.

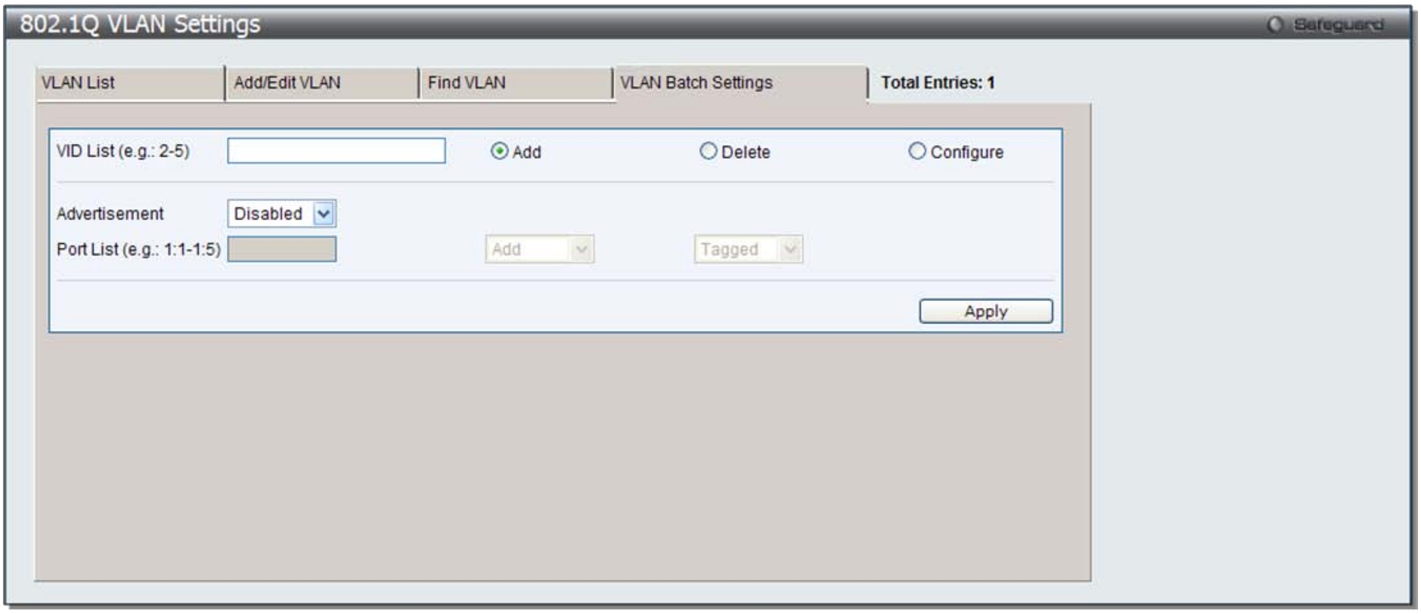

802.1Q VLAN Settings
Safeguard
VLAN List
Add/Edit VLAN
Find VLAN
VLAN Batch Settings
Total Entries: 1
VID List (e.g.: 2-5)
● Add
○ Delete
○ Configure
Advertisement
Disabled
Port List (e.g.: 1:1-1:5)
Add
Tagged
Apply

Figure 4-7 802.1Q VLAN Settings – VLAN Batch Settings Tab window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter a VLAN ID List that can be added, deleted or configured.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port List	Allows an individual port list to be added or deleted as a member of the VLAN.
Tagged	Specify the port as 802.1Q tagged. Use the drop-down menu to designate the port as tagged.
Untagged	Specify the port as 802.1Q untagged. Use the drop-down menu to designate the port as untagged.
Forbidden	Specify the port as not being a member of the VLAN and that the port is forbidden from

	becoming a member of the VLAN dynamically. Use the drop-down menu to designate the port as forbidden.

Click the **Apply** button to accept the changes made.

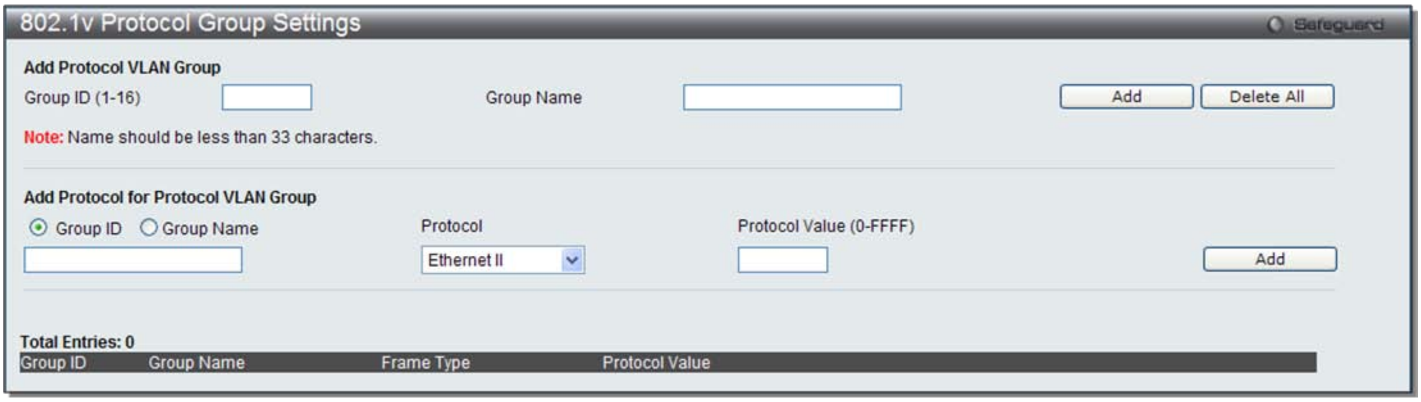
NOTE: The Switch supports up to 4k static VLAN entries.

802.1v Protocol VLAN

802.1v Protocol Group Settings

The user can create Protocol VLAN groups and add protocols to that group. The 802.1v Protocol VLAN Group Settings support multiple VLANs for each protocol and allows the user to configure the untagged ports of different protocols on the same physical port. For example, it allows the user to configure an 802.1Q and 802.1v untagged port on the same physical port. The lower half of the table displays any previously created groups.

To view the following window, click **L2 Features > VLAN > 802.1v protocol VLAN > 802.1v Protocol Group Settings**, as show below:



Note: Name should be less than 33 characters.

Total Entries: 0

Figure 4-8 802.1v Protocol Group Settings window

The fields that can be configured are described below:

Parameter	Description
Group ID (1-16)	Select an ID number for the group, between *1* and *16.*
Group Name	This is used to identify the new Protocol VLAN group. Type an alphanumeric string of up to 32 characters.
Protocol	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. Use the drop-down menu to toggle between *Ethernet II*, *IEEE802.3 SNAP*, and *IEEE802.3 LLC*.
Protocol Value (0-FFFF)	Enter a value for the Group. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is a 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries based on the information entered.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete Settings** button to remove the Protocol for the Protocol VLAN Group information for the specific entry.

Click the **Delete Group** button to remove the entry completely.

NOTE: The Group name value should be less than 33 characters.

802.1v Protocol VLAN Settings

The user can configure Protocol VLAN settings. The lower half of the table displays any previously created settings.

To view the following window, click **L2 Features > VLAN > 802.1v protocol VLAN > 802.1v Protocol VLAN Settings**, as show below:

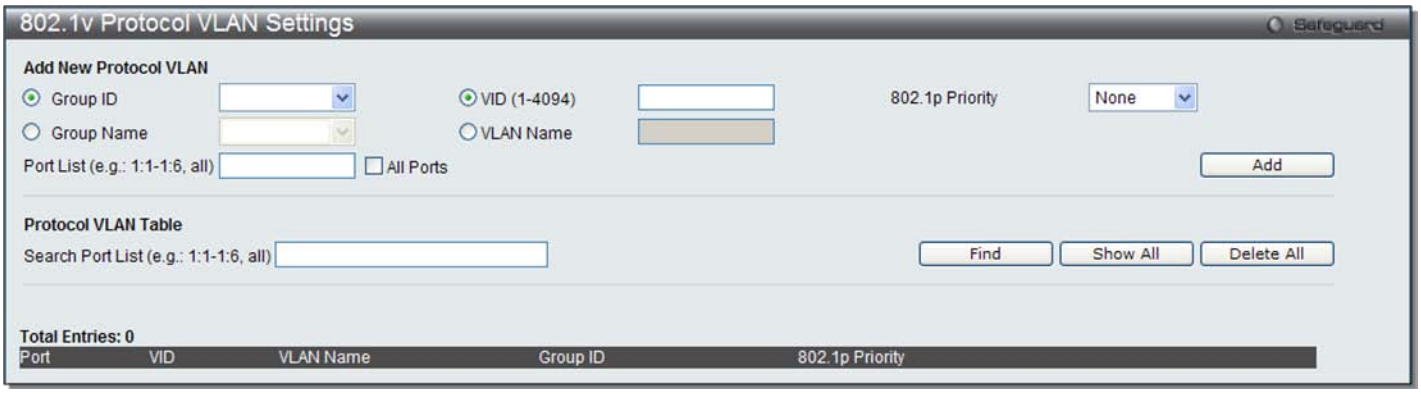

802.1v Protocol VLAN Settings
Safeguard
Add New Protocol VLAN
● Group ID
○ Group Name
Port List (e.g.: 1:1-1:6, all)
☐ All Ports
● VID (1-4094)
○ VLAN Name
802.1p Priority
None
Add
Protocol VLAN Table
Search Port List (e.g.: 1:1-1:6, all)
Find
Show All
Delete All
Total Entries: 0
Port
VID
VLAN Name
Group ID
802.1p Priority

Figure 4-9 802.1v Protocol VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
Group ID	Select a previously configured Group ID from the drop-down menu.
Group Name	Select a previously configured Group Name from the drop-down menu.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to create.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to create.
802.1p Priority	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. Click the corresponding box if you want to set the 802.1p default priority of a packet to the value entered in the Priority (0-7) field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Port List	Select the specified ports you wish to configure by entering the port number in this field, or tick the **All Ports** check box.
Search Port List	This function allows the user to search all previously configured port list settings and display them on the lower half of the table. To search for a port list enter the port number you wish to view and click **Find**. To display all previously configured port lists on the bottom half of the screen click the **Show All** button, to clear all previously configured lists click the **Delete All** button.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Show All** button to display all the Protocol VLANs configured.

Click the **Delete All** button to remove all the entries listed.

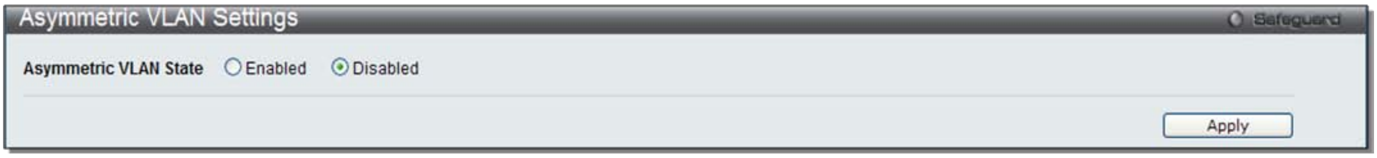
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Asymmetric VLAN Settings

Shared VLAN Learning is a primary example of the requirement for Asymmetric VLANs. Under normal circumstances, a pair of devices communicating in a VLAN environment will both send and receive using the same VLAN; however, there are some circumstances in which it is convenient to make use of two distinct VLANs, one used for A to transmit to B and the other used for B to transmit to A in these cases Asymmetric VLANs are needed. An example of when this type of configuration might be required, would be if the client was on a distinct IP subnet, or if there was some confidentiality-related need to segregate traffic between the clients.

To view this window click **L2 Features > VLAN > Asymmetric VLAN Settings**, as show below:



Asymmetric VLAN State ○ Enabled ● Disabled

Figure 4-10 Asymmetric VLAN Settings window

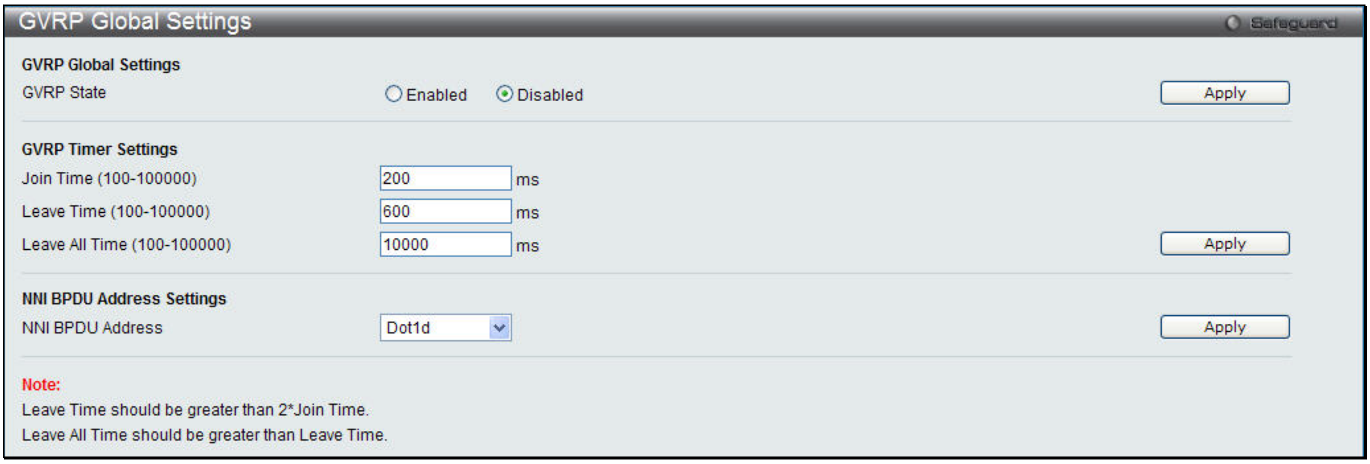
Click **Apply** to implement changes.

GVRP

GVRP Global Settings

Users can determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Global Settings**, as show below:



GVRP State ○ Enabled ● Disabled

Join Time (100-100000) 200 ms

Leave Time (100-100000) 600 ms

Leave All Time (100-100000) 10000 ms

NNI BPDU Address Dot1d

Note:

Leave Time should be greater than 2*Join Time.

Leave All Time should be greater than Leave Time.

Figure 4-11 GVRP Global Settings window

The fields that can be configured are described below:

Parameter	Description
GVRP State	Click the radio buttons to enable or disable the GVRP State.

Join Time (100-100000)	Enter the Join Time value in milliseconds.
Leave Time (100-100000)	Enter the Leave Time value in milliseconds.
Leave All Time (100-100000)	Enter the Leave All Time value in milliseconds.
NNI BPDU Address	Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.

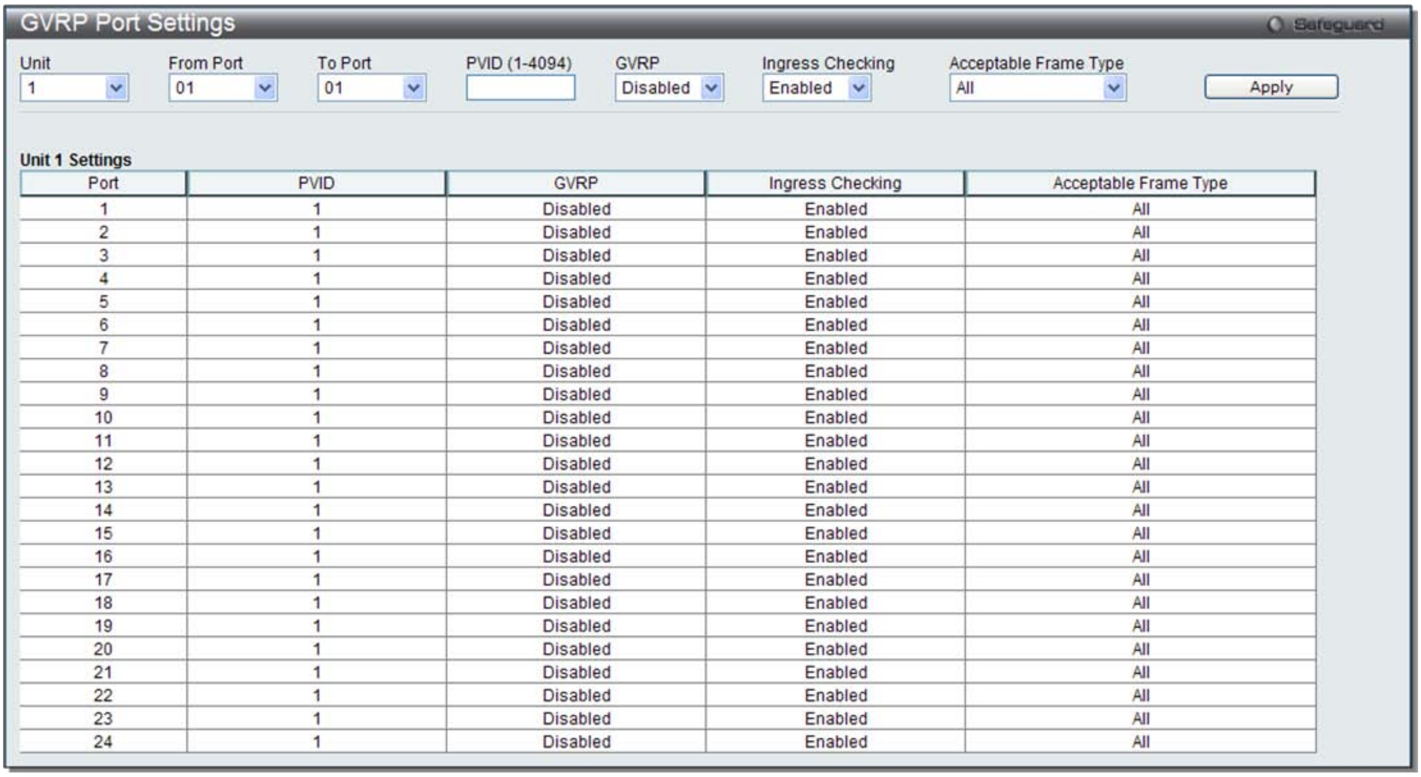
Click the **Apply** button to accept the changes made for each individual section.

NOTE: The **Leave Time** value should be greater than twice the **Join Time** value. The **Leave All Time** value should be greater than the **Leave Time** value.

GVRP Port Settings

On this page the user can configure the GVRP port parameters.

To view the following window, click **L2 Features > VLAN > GVRP > GVRP Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
PVID (1-4094):
GVRP: Disabled
Ingress Checking: Enabled
Acceptable Frame Type: All

Unit 1 Settings

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All
2	1	Disabled	Enabled	All
3	1	Disabled	Enabled	All
4	1	Disabled	Enabled	All
5	1	Disabled	Enabled	All
6	1	Disabled	Enabled	All
7	1	Disabled	Enabled	All
8	1	Disabled	Enabled	All
9	1	Disabled	Enabled	All
10	1	Disabled	Enabled	All
11	1	Disabled	Enabled	All
12	1	Disabled	Enabled	All
13	1	Disabled	Enabled	All
14	1	Disabled	Enabled	All
15	1	Disabled	Enabled	All
16	1	Disabled	Enabled	All
17	1	Disabled	Enabled	All
18	1	Disabled	Enabled	All
19	1	Disabled	Enabled	All
20	1	Disabled	Enabled	All
21	1	Disabled	Enabled	All
22	1	Disabled	Enabled	All
23	1	Disabled	Enabled	All
24	1	Disabled	Enabled	All

Figure 4-12 GVRP Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the starting and ending ports to use.
PVID (1-4094)	This field is used to manually assign a PVID to a VLAN. The Switch's default is to assign all ports to the default VLAN with a VID of 1.The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an

	802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is *Enabled*, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The GARP VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.
Ingress Checking	This drop-down menu allows the user to enable the port to compare the VID tag of an incoming packet with the port VLAN membership. If enable ingress checking and the reception port is not the member port of the frame’s VLAN, the frame shall be discarded.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between *Tagged Only*, which means only VLAN tagged frames will be accepted, and *All*, which mean both tagged and untagged frames will be accepted. *All* is enabled by default.

Click the **Apply** button to accept the changes made.

MAC-based VLAN Settings

Users can create new MAC-based VLAN entries, search and delete existing entries. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN.

To view the following window, click **L2 Features > VLAN > MAC-based VLAN Settings**, as show below:

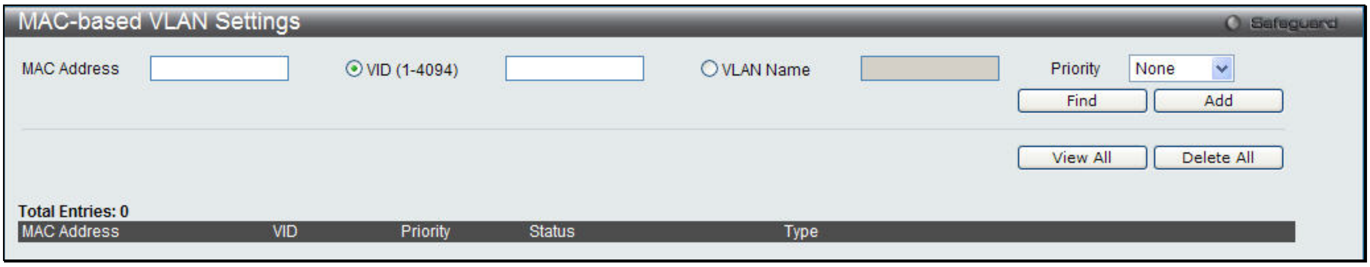


Figure 4-13 MAC-based VLAN Settings

The fields that can be configured are described below:

Parameter	Description
MAC Address	Specify the MAC address.
VID (1-4094)	Select this option and enter the VLAN ID.
VLAN Name	Select this option and enter the VLAN name of a previously configured VLAN.
Priority	Specify the priority that assigns to untagged packets.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

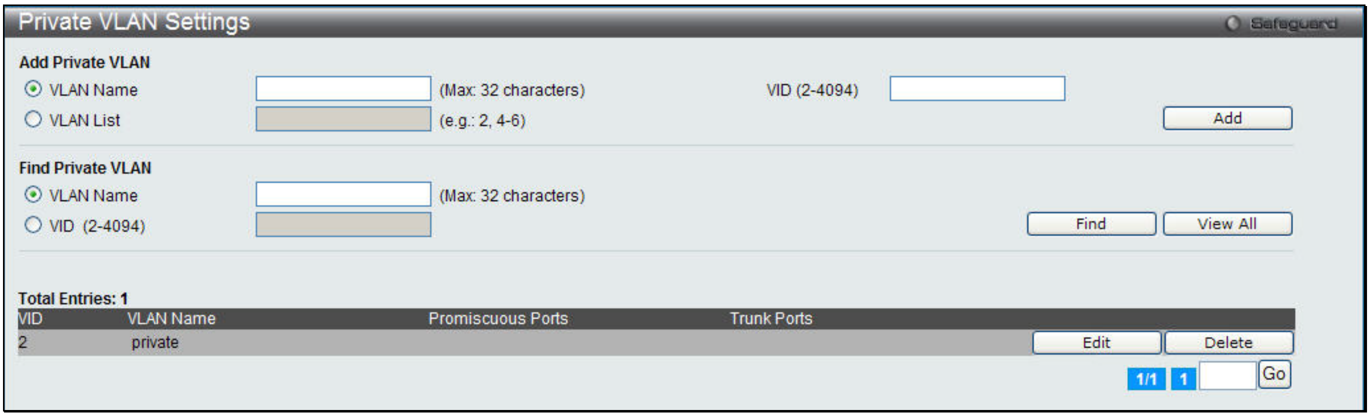
Private VLAN Settings

A private VLAN is comprised of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. A private VLAN ID is presented by the VLAN ID of the primary VLAN. The command used to associate or de-associate a secondary VLAN with a primary VLAN.

A secondary VLAN cannot be associated with multiple primary VLANs. The untagged member port of the primary VLAN is named as the promiscuous port. The tagged member port of the primary VLAN is named as the trunk port. A promiscuous port of a private VLAN cannot be promiscuous port of other private VLANs. The primary VLAN member port cannot be a secondary VLAN member at the same time, or vice versa. A secondary VLAN can only have the untagged member port. The member port of a secondary VLAN cannot be member port of other secondary VLAN at the same time. When a VLAN is associated with a primary VLAN as the secondary VLAN, the promiscuous port of the primary VLAN will behave as the untagged member of the secondary VLAN, and the trunk port of the primary VLAN will behave as the tagged member of the secondary VLAN. A secondary VLAN cannot be specified with advertisement. Only the primary VLAN can be configured as a layer 3 interface. The private VLAN member port cannot be configured with the traffic segmentation function.

This window allows the user to configure the private VLAN parameters.

To view the following window, click **L2 Features > VLAN > Private VLAN Settings**, as show below:


Private VLAN Settings
Safeguard
Add Private VLAN
● VLAN Name
○ VLAN List
(Max: 32 characters)
(e.g.: 2, 4-6)
VID (2-4094)
Add
Find Private VLAN
● VLAN Name
○ VID (2-4094)
(Max: 32 characters)
Find
View All
Edit
Delete
1/1
1
Go

Total Entries: 1

VID	VLAN Name	Promiscuous Ports	Trunk Ports
2	private		

Figure 4-14 Private VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter a VLAN name.
VID (2-4094)	Enter a VID value.
VLAN List	Enter a list of VLAN ID.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

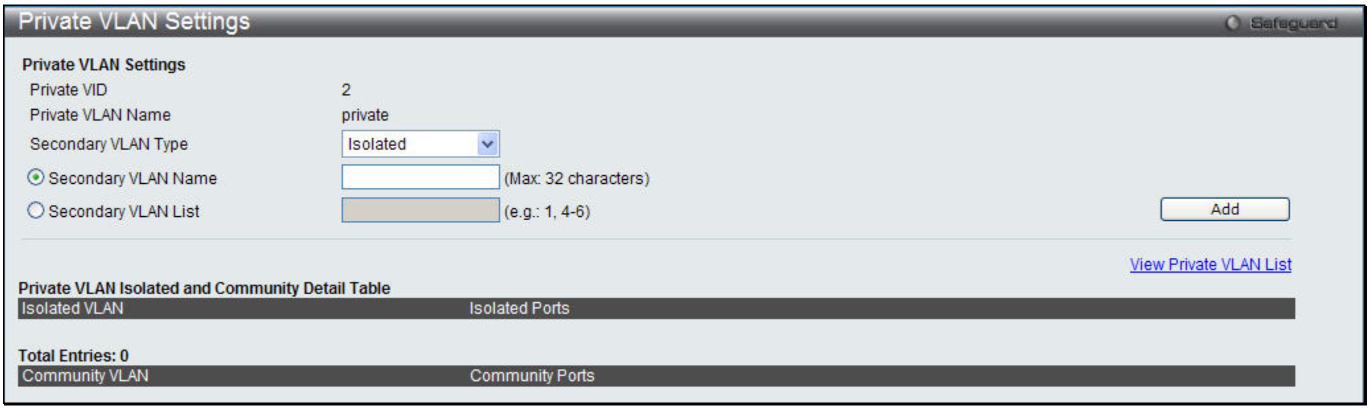
Click the **View All** button to display all the existing entries.

Click the **Edit** button to configure the secondary VLAN.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Click the **Edit** button to see the following window.


Private VLAN Settings
Safeguard
Private VLAN Settings
● Secondary VLAN Name
○ Secondary VLAN List
(Max: 32 characters)
(e.g.: 1, 4-6)
Add
View Private VLAN List

Private VID: 2
Private VLAN Name: private
Secondary VLAN Type: Isolated

Private VLAN Isolated and Community Detail Table

Isolated VLAN	Isolated Ports

Total Entries: 0

Community VLAN	Community Ports

Figure 4-15 Private VLAN Settings - Edit window

The fields that can be configured are described below:

Parameter	Description
Secondary VLAN Type	Use the drop-down menu to select secondary VLAN type between *Isolated* or *Community*.
Secondary VLAN Name	Enter a secondary VLAN name.
Secondary VLAN List	Enter a list of secondary VLAN ID.

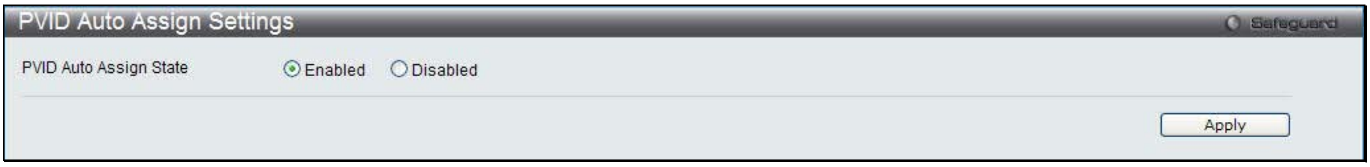
Click the **Add** button to add a new entry based on the information entered.

Click the View Private VLAN List link to view all the private VLAN.

PVID Auto Assign Settings

Users can enable or disable PVID Auto Assign Status. The default setting is enabled.

To view the following window, click **L2 Features > VLAN > PVID Auto Assign Settings**, as show below:



PVID Auto Assign State ● Enabled ○ Disabled

Figure 4-16 PVID Auto Assign Settings window

Click the **Apply** button to accept the changes made.

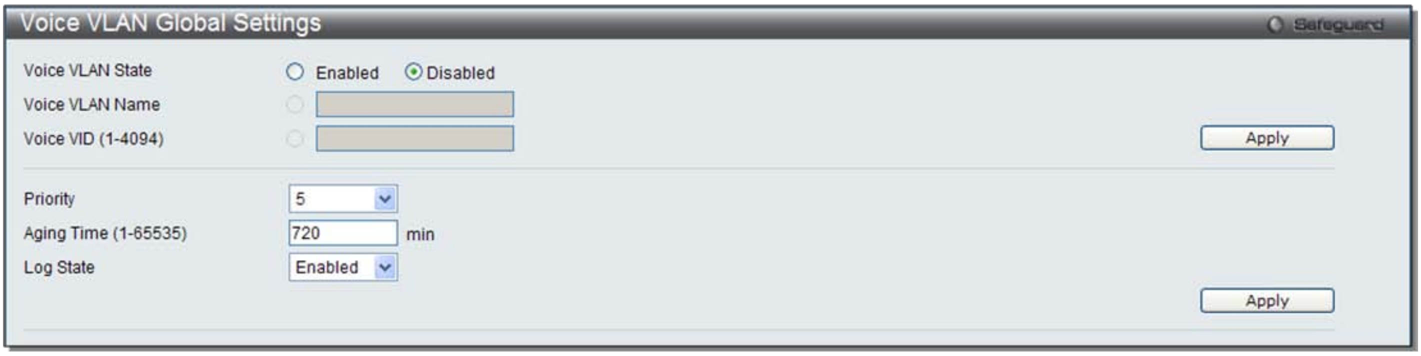
Voice VLAN

Voice VLAN Global Settings

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global Settings**, as show below:



Voice VLAN State ○ Enabled ● Disabled

Voice VLAN Name ○

Voice VID (1-4094) ○

Priority 5

Aging Time (1-65535) 720 min

Log State Enabled

Figure 4-17 Voice VLAN Global Settings window

The fields that can be configured are described below:

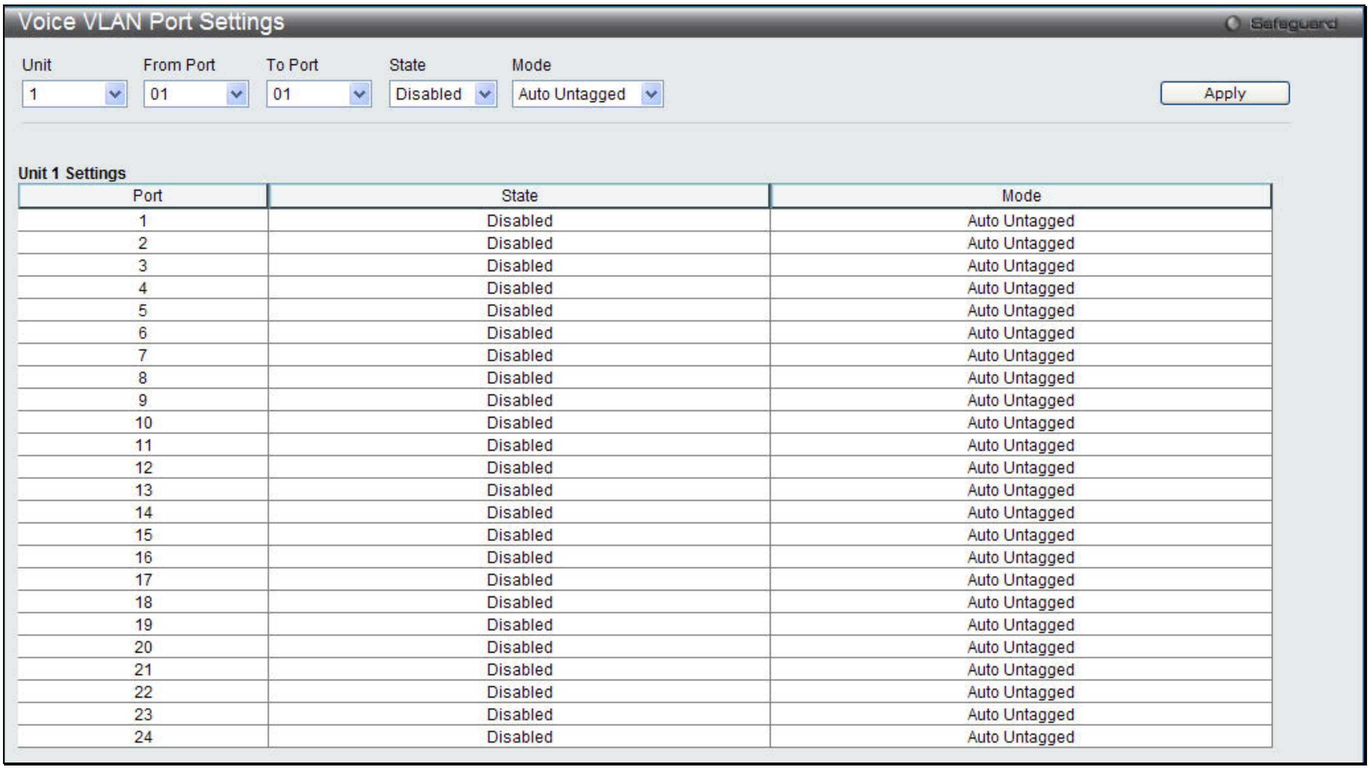
Parameter	Description
Voice VLAN State	The state of the voice VLAN.
Voice VLAN Name	The name of the voice VLAN.
Voice VID (1-4094)	The VLAN ID of the voice VLAN.
Priority	The priority of the voice VLAN, the range is 0 – 7. The default priority is 5.
Aging Time (1-65535)	The aging time to set, the range is 1 – 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.
Log State	Used to enable/disable sending of issue of voice VLAN log.

Click the **Apply** button to accept the changes made for each individual section.

Voice VLAN Port Settings

This page is used to show the ports voice VLAN information.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
State: Disabled
Mode: Auto Untagged

Unit 1 Settings

Port	State	Mode
1	Disabled	Auto Untagged
2	Disabled	Auto Untagged
3	Disabled	Auto Untagged
4	Disabled	Auto Untagged
5	Disabled	Auto Untagged
6	Disabled	Auto Untagged
7	Disabled	Auto Untagged
8	Disabled	Auto Untagged
9	Disabled	Auto Untagged
10	Disabled	Auto Untagged
11	Disabled	Auto Untagged
12	Disabled	Auto Untagged
13	Disabled	Auto Untagged
14	Disabled	Auto Untagged
15	Disabled	Auto Untagged
16	Disabled	Auto Untagged
17	Disabled	Auto Untagged
18	Disabled	Auto Untagged
19	Disabled	Auto Untagged
20	Disabled	Auto Untagged
21	Disabled	Auto Untagged
22	Disabled	Auto Untagged
23	Disabled	Auto Untagged
24	Disabled	Auto Untagged

Figure 4-18 Voice VLAN Port Settings window

The fields that can be configured are described below:

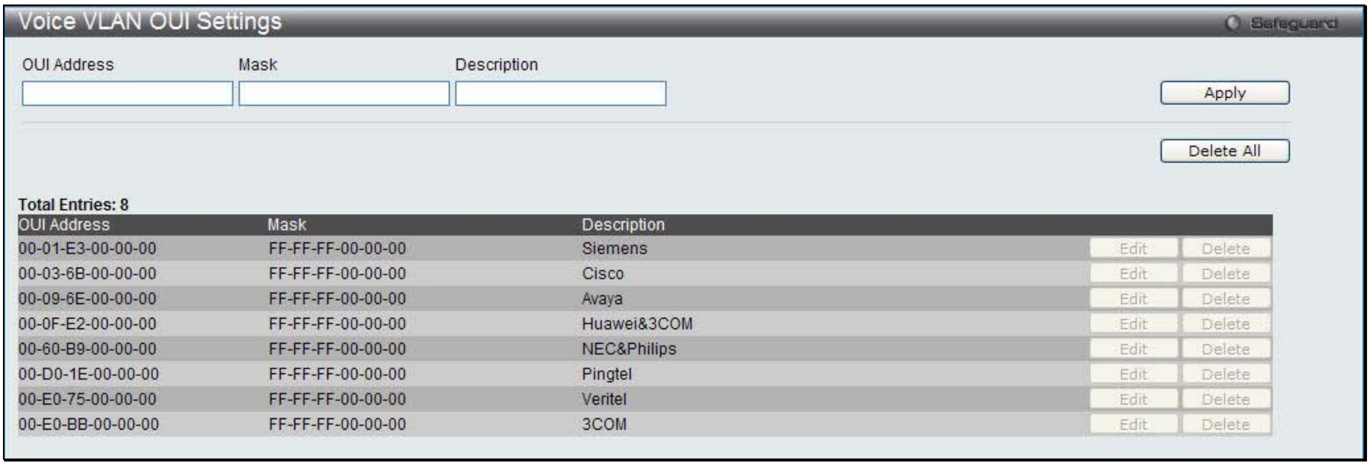
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select a range of port to display.
State	Use the drop-down menu to enable or disable the state of the port.
Mode	Use the drop-down menu to configure the mode of the port.

Click the **Apply** button to accept the changes made.

Voice VLAN OUI Settings

This page is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI** Settings, as show below:



Total Entries: 8

OUI Address	Mask	Description		
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Edit	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Edit	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Edit	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Edit	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Edit	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Edit	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Edit	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Edit	Delete

Figure 4-19 Voice VLAN OUI Settings window

The fields that can be configured are described below:

Parameter	Description
OUI Address	User defined OUI MAC address.
Mask	User defined OUI MAC address mask.
Description	The description for the user defined OUI.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

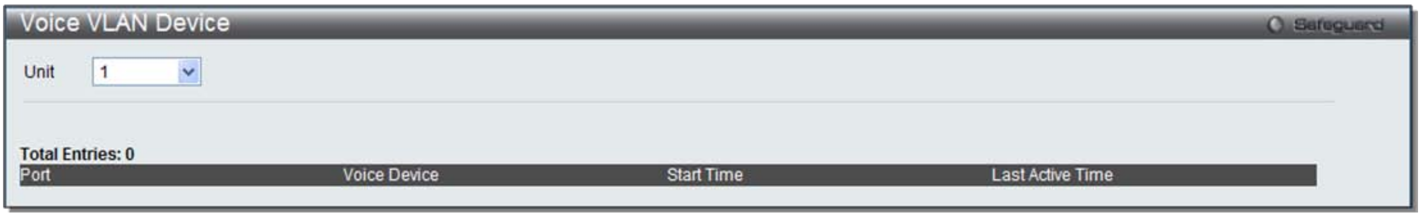
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Voice VLAN Device

This page is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device**, as show below:



Unit: 1

Total Entries: 0

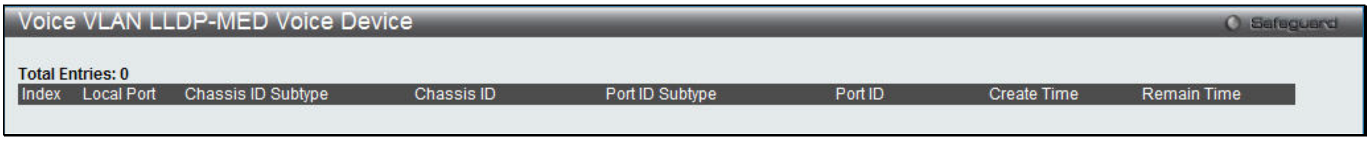
Port	Voice Device	Start Time	Last Active Time

Figure 4-20 Voice VLAN Device window

Voice VLAN LLDP-MED Voice Device

This window is used to show the voice devices being discovered by the LLDP-MED.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Voice Device**, as show below:



Voice VLAN LLDP-MED Voice Device

Total Entries: 0

Index	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Create Time	Remain Time

Figure 4-21 Voice VLAN LLDP-MED Voice Device window

VLAN Trunk Settings

Enable VLAN on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without a VLAN Trun**k**, you must first configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with VLAN Trunk enabled on a port(s) in each intermediary switch, you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Refer to the following figure for an illustrated example.

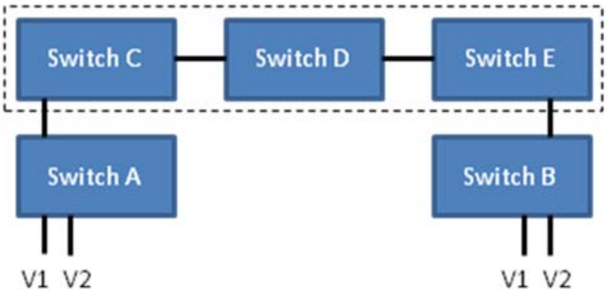
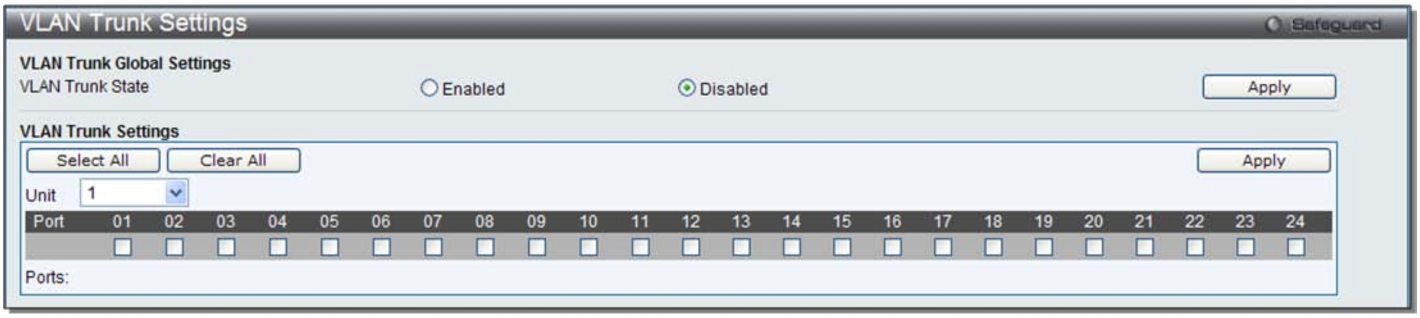


Figure 4-22 Example of VLAN Trunk

Users can combine a number of VLAN ports together to create VLAN trunks.

To view the following window, click **L2 Features > VLAN > VLAN Trunk Settings**, as show below:



VLAN Trunk Settings

VLAN Trunk Global Settings

VLAN Trunk State ○ Enabled ● Disabled

VLAN Trunk Settings

Unit: 1

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Ports:

Figure 4-23 VLAN Trunk Settings window

The fields that can be configured are described below:

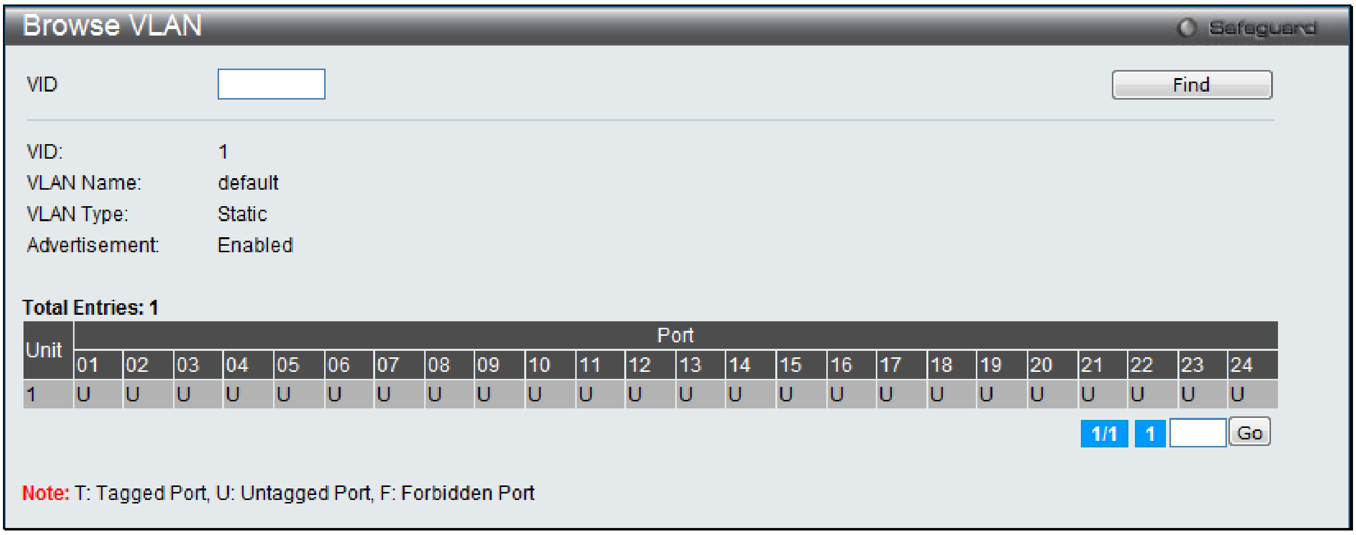
Parameter	Description
VLAN Trunk State	Enable or disable the VLAN trunking global state.
Unit	Select the unit you want to configure.
Ports	The ports to be configured. By clicking the **Select All** button, all the ports will be included. By clicking the **Clear All** button, all the ports will not be included.

Click the **Apply** button to accept the changes made for each individual section.

BROWSE VLAN

Users can display the VLAN status for each of the Switch's ports viewed by VLAN. Enter a VID (VLAN ID) in the field at the top of the window and click the **Find** button.

To view the following window, click **L2 Features > VLAN > Browse VLAN**, as show below:



VID: 1
VLAN Name: default
VLAN Type: Static
Advertisement: Enabled

Total Entries: 1

Unit	Port																						
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Note: T: Tagged Port, U: Untagged Port, F: Forbidden Port

Figure 4-24 Browse VLAN window

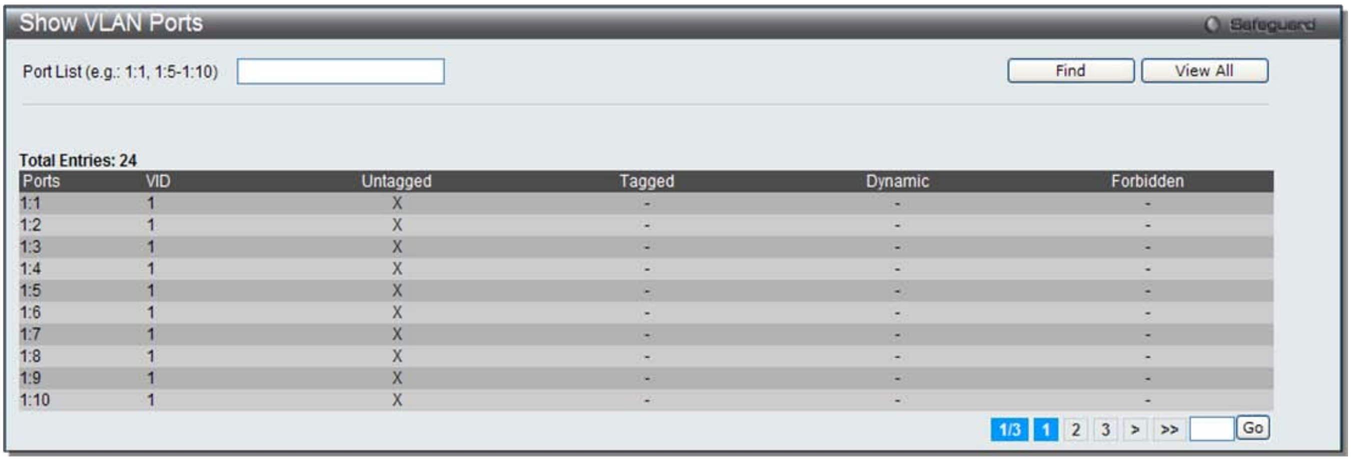
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE: The abbreviations used on this page are **Tagged Port (T)**, **Untagged Port (U)** and **Forbidden Port (F)**.

SHOW VLAN PORTS

Users can display the VLAN ports of the Switch's viewed by VID. Enter a Port or a **Port List** in the field at the top of the window and click the **Find** button.

To view the following window, click **L2 Features > VLAN > Show VLAN Ports**, as show below:



Total Entries: 24

Ports	VID	Untagged	Tagged	Dynamic	Forbidden
1:1	1	X	-	-	-
1:2	1	X	-	-	-
1:3	1	X	-	-	-
1:4	1	X	-	-	-
1:5	1	X	-	-	-
1:6	1	X	-	-	-
1:7	1	X	-	-	-
1:8	1	X	-	-	-
1:9	1	X	-	-	-
1:10	1	X	-	-	-

Figure 4-25 Show VLAN Ports window

Click the **View All** button to display all the existing entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

QinQ (EI Mode Only)

Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Double VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Double VLAN tagged packet.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Consider the example below:

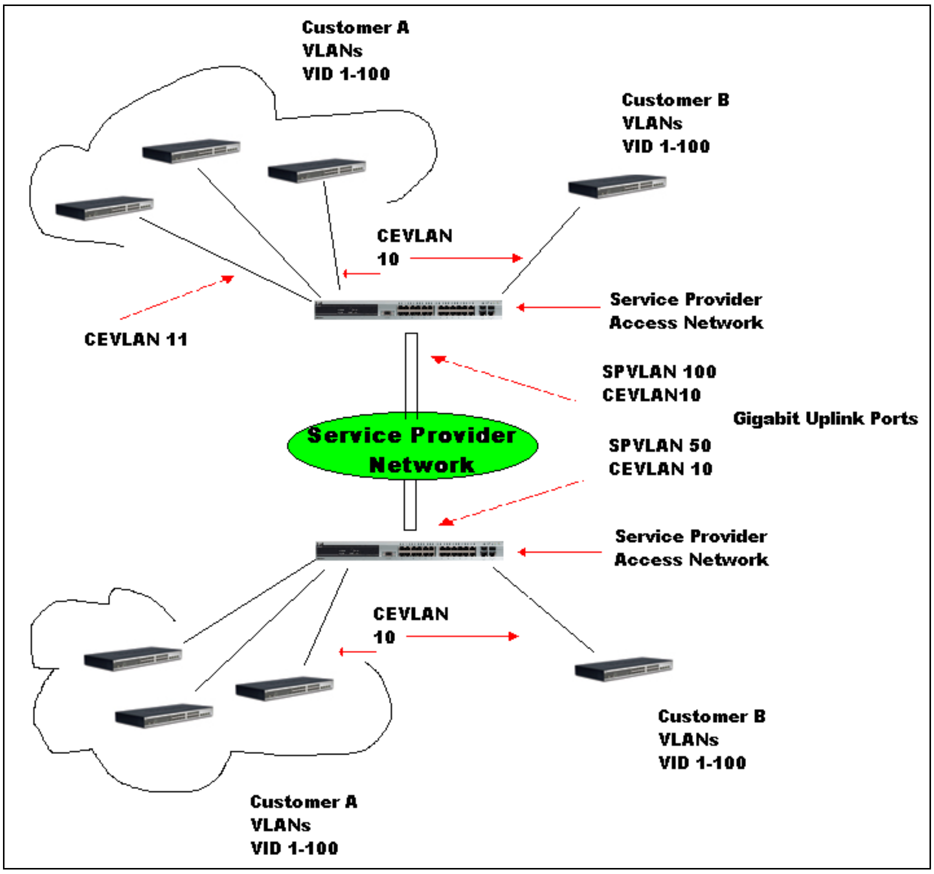

Customer A
VLANs
VID 1-100
Customer B
VLANs
VID 1-100
CEVLAN
10
CEVLAN 11
Service Provider
Access Network
SPVLAN 100
CEVLAN10
Gigabit Uplink Ports
Service Provider
Network
SPVLAN 50
CEVLAN 10
Service Provider
Access Network
CEVLAN
10
Customer B
VLANs
VID 1-100
Customer A
VLANs
VID 1-100

Figure 4-26 QinQ example window

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs), 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way, the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SPVLAN, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Double VLANs

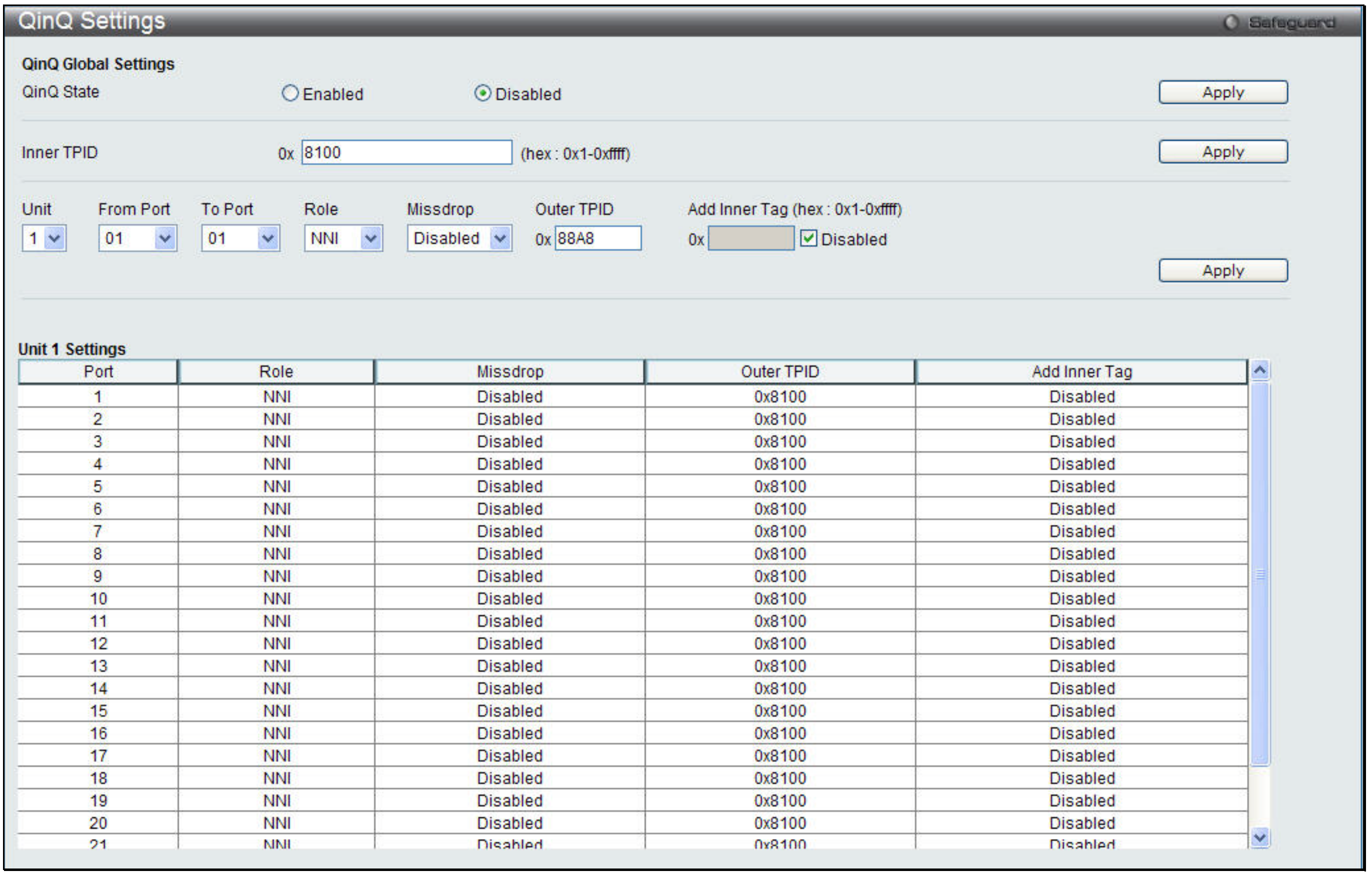
Some rules and regulations apply with the implementation of the Double VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Once Double VLANs are enabled, GVRP must be disabled.
7. All packets sent from the CPU to the Access ports must be untagged.
8. The following functions will not operate when the switch is in Double VLAN mode:
    - Guest VLANs.
    - Web-based Access Control.
    - IP Multicast Routing.
    - GVRP.
    - All Regular 802.1Q VLAN functions.

QinQ Settings

This window is used to configure the Q-in-Q parameters.

To view the following window, click **L2 Features > QinQ > QinQ Settings**, as show below:



QinQ Global Settings

QinQ State ○ Enabled ● Disabled

Inner TPID 0x 8100 (hex : 0x1-0xffff)

Unit	From Port	To Port	Role	Missdrop	Outer TPID	Add Inner Tag (hex : 0x1-0xffff)
1	01	01	NNI	Disabled	0x 88A8	0x ☑ Disabled

Unit 1 Settings

Port	Role	Missdrop	Outer TPID	Add Inner Tag
1	NNI	Disabled	0x8100	Disabled
2	NNI	Disabled	0x8100	Disabled
3	NNI	Disabled	0x8100	Disabled
4	NNI	Disabled	0x8100	Disabled
5	NNI	Disabled	0x8100	Disabled
6	NNI	Disabled	0x8100	Disabled
7	NNI	Disabled	0x8100	Disabled
8	NNI	Disabled	0x8100	Disabled
9	NNI	Disabled	0x8100	Disabled
10	NNI	Disabled	0x8100	Disabled
11	NNI	Disabled	0x8100	Disabled
12	NNI	Disabled	0x8100	Disabled
13	NNI	Disabled	0x8100	Disabled
14	NNI	Disabled	0x8100	Disabled
15	NNI	Disabled	0x8100	Disabled
16	NNI	Disabled	0x8100	Disabled
17	NNI	Disabled	0x8100	Disabled
18	NNI	Disabled	0x8100	Disabled
19	NNI	Disabled	0x8100	Disabled
20	NNI	Disabled	0x8100	Disabled
21	NNI	Disabled	0x8100	Disabled

Figure 4-27 QinQ Settings Window

The fields that can be configured are described below:

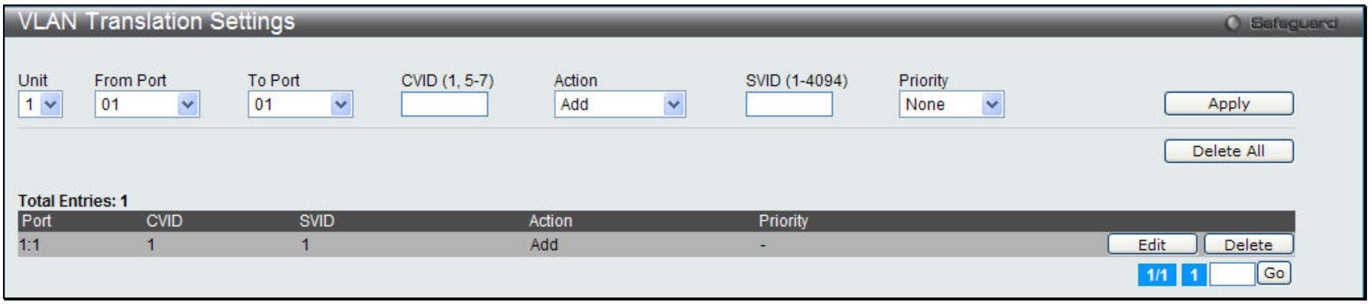
Parameter	Description
QinQ State	Click to enable or disable the Q-in-Q state.
Inner TPID	Enter an Inner TPID in SP-VLAN tag here.
Unit	Specifies the unit ID to be configured.
From Port / To Port	Use the drop-down menus to select a range of ports to use in the configuration.
Role	Port role in Q-in-Q mode, it can be UNI port or NNI port
Missdrop	This option enables or disables C-VLAN based SP-VLAN assignment miss drop. If Missdrop is enabled, the packet that does not match any assignment rule in the Q-in-Q profile will be dropped. If disabled, then the packet will be forwarded and will be assigned to the PVID of the received port.
Outer TPID	Enter an Outer TPID in SP-VLAN tag here.
Add Inner Tag	Specifies that an Inner Tag will be added to the entry. By default the **Disabled** option is selected.

Click the **Apply** button to accept the changes made for each individual section.

VLAN Translation Settings

This window is used to add translation relationship between C-VLAN and SP-VLAN. On ingress at UNI port, the C-VLAN tagged packets will be translated to SP-VLAN tagged packets by adding or replacing according the configured rule. On egress at this port, the SP-VLAN tag will be recovered to C-VLAN tag or be striped. The priority will be the priority in the SP-VLAN tag if the inner priority flag is disabled for the receipt port.

To view the following window, click **L2 Features > QinQ > VLAN Translation Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
CVID (1, 5-7):
Action: Add
SVID (1-4094):
Priority: None

Total Entries: 1

Port	CVID	SVID	Action	Priority
1:1	1	1	Add	-

1/1 1

Figure 4-28 VLAN Translation Settings Window

The fields that can be configured are described below:

Parameter	Description
Unit	Specifies the unit ID to be configured.
From Port / To Port	Use the drop-down menus to select a range of ports to use in the configuration.
CVID (1, 5-7)	Enter the C-VLAN ID to match.
Action	The action indicates to add an S-tag before a C-tag or to replace the original C-tag by an S-tag.
SVID (1-4094)	Enter the SP-VLAN ID.
Priority	Use the drop-down menu to select the priority of the s-tag.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Delete All** button to remove all the entries listed.

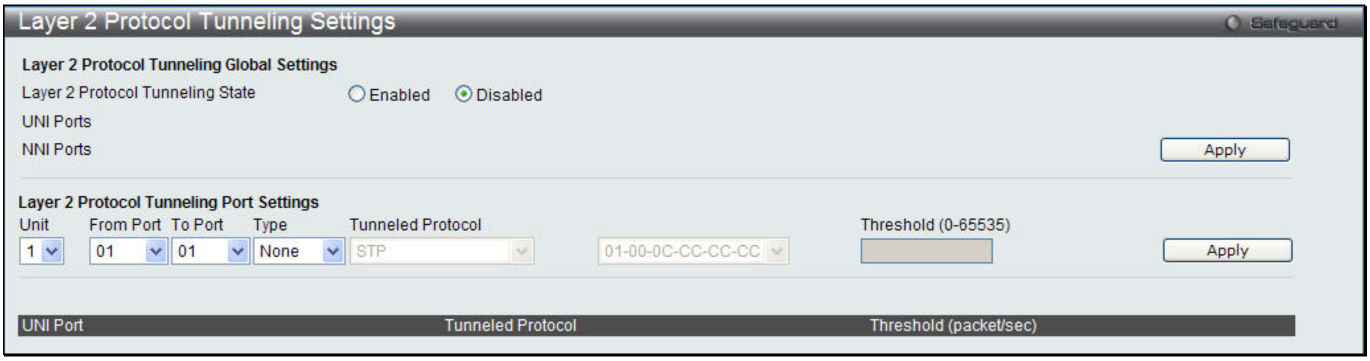
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove a specific entry.

Layer 2 Protocol Tunneling Settings

This window is used to configure Layer 2 protocol tunneling settings.

To view the following window, click **L2 Features > Layer 2 Protocol tunneling Settings**, as show below:



Layer 2 Protocol Tunneling Global Settings

Layer 2 Protocol Tunneling State ○ Enabled ● Disabled

UNI Ports

NNI Ports

Layer 2 Protocol Tunneling Port Settings

Unit	From Port	To Port	Type	Tunneled Protocol		Threshold (0-65535)
1	01	01	None	STP	01-00-0C-CC-CC-CC	

UNI Port	Tunneled Protocol	Threshold (packet/sec)

Figure 4-29 Layer 2 Protocol Tunneling Settings window

The fields that can be configured are described below:

Parameter	Description
Layer 2 Protocol Tunneling State	Click to enable or disable the Layer 2 protocol tunneling state.
Unit	Specifies the unit ID to be configured.
From Port / To Port	Use the drop-down menus to select a range of ports to use in the configuration.
Type	Specify the type of the ports. *UNI* - Specify the ports as UNI ports. *NNI* - Specify the ports as NNI ports. *None* - Disable tunnel on it.
Tunneled Protocol	Specify tunneled protocols on the UNI ports. *STP* - Specify to use the STP protocol. *GVRP* - Specify to use the GVRP protocol. *Protocol MAC* - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. The MAC address can be 01-00-0C-CC-CC-CC or 01-00-0C-CC-CC-CD. *All* - All tunnel enabled Layer 2 protocols will be tunneled on the ports.
Threshold (0-65535)	Specify the drop threshold for packets-per-second accepted on the UNI ports. The ports drop the PDU if the protocol’s threshold is exceeded.

Click the **Apply** button to accept the changes made for each individual section.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance.

Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1D-1998 and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning

Disabled	Disabled	Disabled	No	No
Discarding	*Discarding*	*Blocking*	No	No
Discarding	*Discarding*	*Listening*	No	No
Learning	*Learning*	*Learning*	No	**Yes**
Forwarding	**Forwarding**	**Forwarding**	**Yes**	**Yes**

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

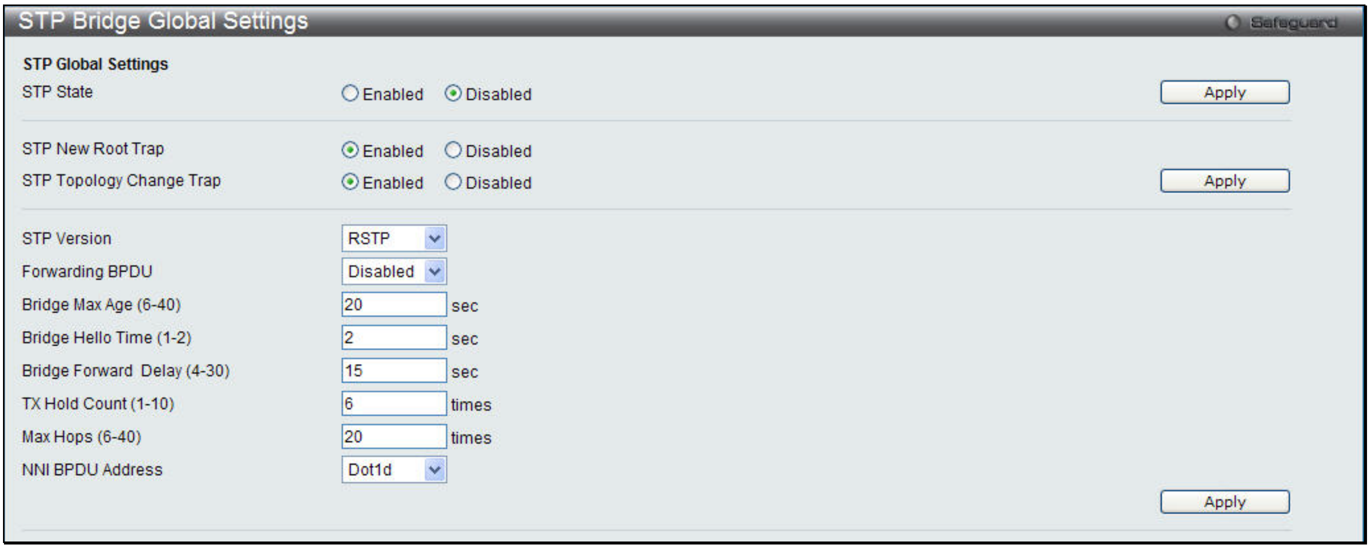
The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per-user-defined group of ports basis.

STP Bridge Global Settings

On this page the user can configure the STP bridge global parameters.

To view the following window, click **L2 Features > Spanning Tree > STP Bridge Global Settings**, as show below:


STP Bridge Global Settings

STP Global Settings

STP State ○ Enabled ● Disabled

STP New Root Trap ● Enabled ○ Disabled

STP Topology Change Trap ● Enabled ○ Disabled

STP Version	RSTP
Forwarding BPDU	Disabled
Bridge Max Age (6-40)	20 sec
Bridge Hello Time (1-2)	2 sec
Bridge Forward Delay (4-30)	15 sec
TX Hold Count (1-10)	6 times
Max Hops (6-40)	20 times
NNI BPDU Address	Dot1d

Figure 4-30 STP Bridge Global Settings window

The fields that can be configured are described below:

Parameter	Description
STP State	Use the radio button to globally enable or disable STP.
STP new Root Trap	Click to enable or disable sending new root traps.
STP Topology Change Trap	Click to enable or disable sending topology change traps.
STP Version	Use the drop-down menu to choose the desired version of STP: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *MSTP* - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Forwarding BPDU	This field can be *Enabled* or *Disabled.* When *Enabled,* it allows the forwarding of STP BPDU packets from other network devices. The default is *Enabled*.
Bridge Max Age (6-40)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. The user may choose a time between *6* and *40* seconds. The default value is *20* seconds.
Bridge Hello Time (1-2)	The Hello Time can be set from *1* to *2* seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. The default is *2* seconds.
Bridge Forward Delay (4-30)	The Forward Delay can be from *4* to *30* seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state. The default is *15* seconds
Tx Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.
Max Hops (6-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from *6* to *40*. The

	default is *20*.
NNI BPDU Address	Used to determine the BPDU protocol address for GVRP in service provide site. It can use 802.1d GVRP address, 802.1ad service provider GVRP address or a user defined multicast address. The range of the user defined address is 0180C2000000 - 0180C2FFFFFF.

Click the **Apply** button to accept the changes made for each individual section.

NOTE: The Bridge Hello Time cannot be longer than the Bridge Max Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

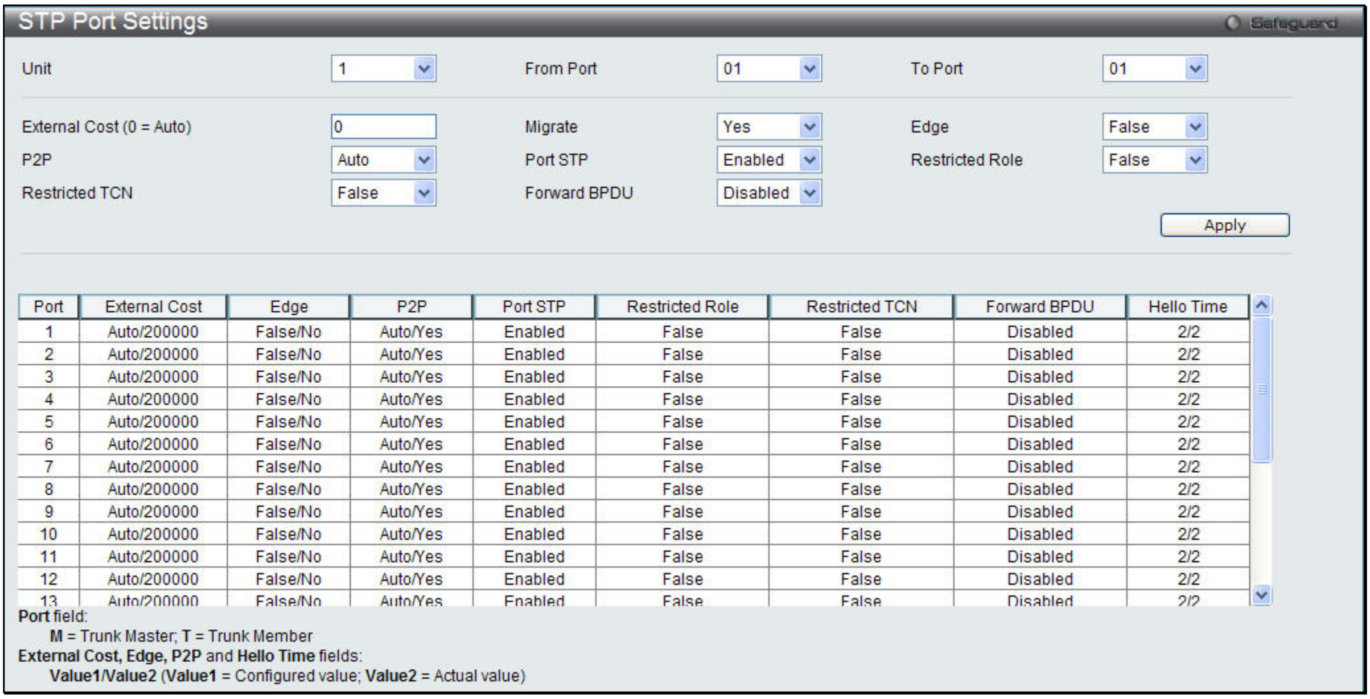
Bridge Max Age <= 2 x (Bridge Forward Delay - 1 second)

Bridge Max Age > 2 x (Bridge Hello Time + 1 second)

STP Port Settings

STP can be set up on a port per port basis. It is advisable to define an STP Group to correspond to a VLAN group of ports.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
External Cost (0 = Auto): 0
Migrate: Yes
Edge: False
P2P: Auto
Port STP: Enabled
Restricted Role: False
Restricted TCN: False
Forward BPDU: Disabled

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	Hello Time
1	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
2	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
3	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
4	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
5	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
6	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
7	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
8	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
9	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
10	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
11	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
12	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2
13	Auto/200000	False/No	Auto/Yes	Enabled	False	False	Disabled	2/2

Port field:
M = Trunk Master; **T** = Trunk Member
External Cost, Edge, P2P and **Hello Time** fields:
Value1/Value2 (**Value1** = Configured value; **Value2** = Actual value)

Figure 4-31 STP Port Settings window

The fields that can be configured are described below:

Parameter	**Description**
Unit	Select the unit you want to configure.
From Port / To Port	Select the starting and ending ports to be configured.
External Cost (0=Auto)	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto). Setting *0* for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is *200000* and the default port cost for a Gigabit port is *20000*. Enter a value between *1* and *200000000* to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
P2P	Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports

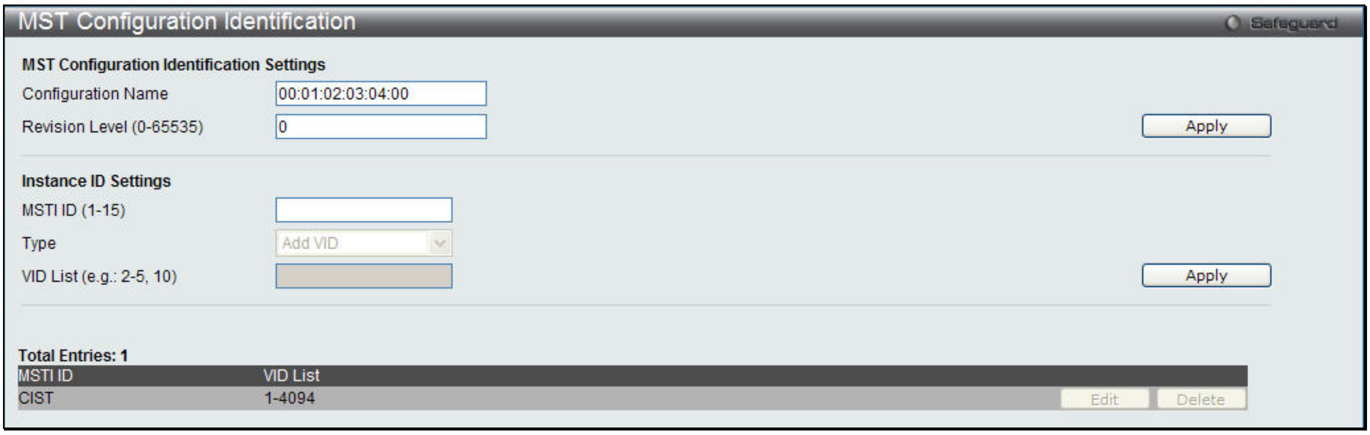
	are similar to edge ports; however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A P2P value of *False* indicates that the port cannot have P2P status. *Auto* allows the port to have P2P status whenever possible and operate as if the P2P status were *True*. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the P2P status changes to operate as if the P2P value were *False*. The default setting for this parameter is *Auto*.
Restricted TCN	Topology Change Notification is a simple BPDU that a bridge sends out to its root port to signal a topology change. Restricted TCN can be toggled between *True* and *False*. If set to *True*, this stops the port from propagating received topology change notifications and topology changes to other ports. The default is *False*.
Migrate	When operating in RSTP mode, selecting *Yes* forces the port that has been selected to transmit RSTP BPDUs.
Port STP	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is *Enabled*.
Forward BPDU	Use the drop-down menu to enable or disable the flooding of BPDU packets when STP is disabled.
Edge	Choosing the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the *False* parameter indicates that the port does not have edge port status. Alternatively, the *Auto* option is available.
Restricted Role	Use the drop-down menu to toggle Restricted Role between *True* and *False*. If set to *True*, the port will never be selected to be the Root port. The default is *False*.

Click the **Apply** button to accept the changes made.

MST Configuration Identification

This window allows the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one CIST, or Common Internal Spanning Tree, of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

To view the following window, click **L2 Features > Spanning Tree > MST Configuration Identification**, as show below:



MST Configuration Identification Settings

Configuration Name: 00:01:02:03:04:00

Revision Level (0-65535): 0

Instance ID Settings

MSTI ID (1-15):

Type: Add VID

VID List (e.g.: 2-5, 10):

Total Entries: 1

MSTI ID	VID List
CIST	1-4094

Figure 4-32 MST Configuration Identification window

The fields that can be configured are described below:

Parameter	Description
Configuration Name	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). If a Configuration Name is not set, this field will show the MAC address to the device running MSTP.

Revision Level (0-65535)	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch.
MSTI ID (1-15)	Enter a number between *1* and *15* to set a new MSTI on the Switch.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices: *Add VID* - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. *Remove VID* - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number *1* to *4094*.

Click the **Apply** button to accept the changes made for each individual section.

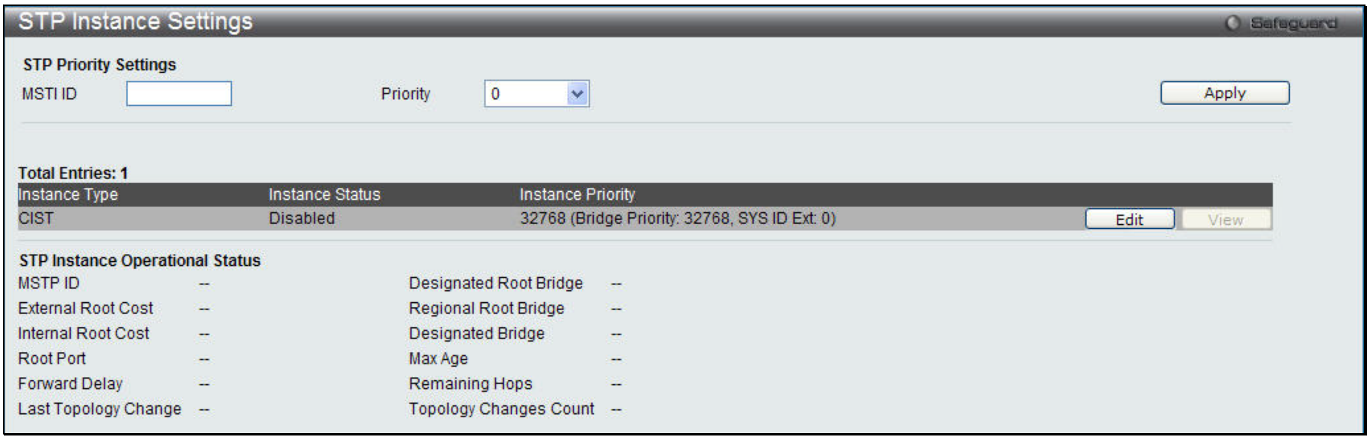
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

STP Instance Settings

This window displays MSTIs currently set on the Switch and allows users to change the Priority of the MSTIs.

To view the following window, click **L2 Features > Spanning Tree > STP Instance Settings**, as show below:



MSTI ID
Priority 0

Total Entries: 1

Instance Type	Instance Status	Instance Priority
CIST	Disabled	32768 (Bridge Priority: 32768, SYS ID Ext: 0)

STP Instance Operational Status

MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max Age	--
Forward Delay	--	Remaining Hops	--
Last Topology Change	--	Topology Changes Count	--

Figure 4-33STP Instance Settings window

The fields that can be configured are described below:

Parameter	Description
MSTI ID	Enter the MSTI ID in this field. An entry of *0* denotes the CIST (default MSTI).
Priority	Enter the priority in this field. The available range of values is from *0* to *61440*.

Click the **Apply** button to accept the changes made.

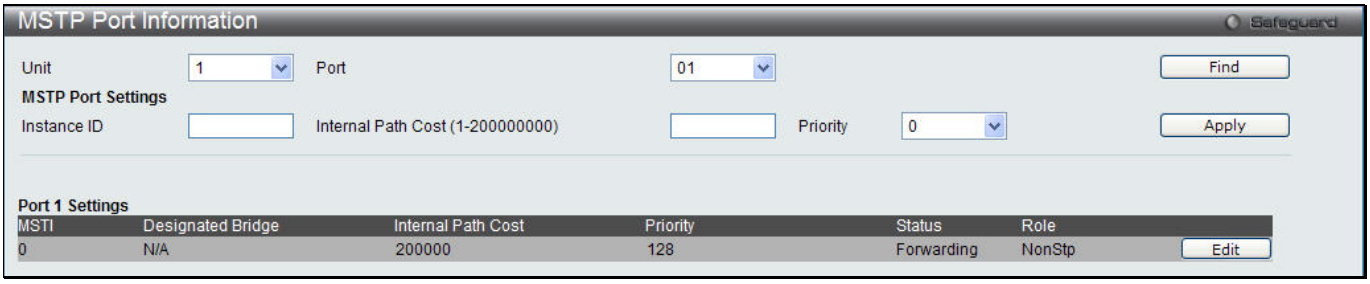
Click the **Edit** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

MSTP Port Information

This window displays the current MSTI configuration information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **L2 Features > Spanning Tree > MSTP Port Information**, as show below:



Unit: 1
Port: 01

MSTP Port Settings

Instance ID:
Internal Path Cost (1-200000000):
Priority: 0

Port 1 Settings

MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role	
0	N/A	200000	128	Forwarding	NonStp	Edit

Figure 4-34 MSTP Port Information window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Select the port you want to configure.
Instance ID	The MSTI ID of the instance to be configured. Enter a value between *0* and *15*. An entry of *0* in this field denotes the CIST (default MSTI).
Internal Path Cost (1-200000000)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of *1* to *200000000* will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission. Selecting *0* (zero) for this parameter will set the quickest route automatically and optimally for an interface.
Priority	Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click the **Find** button to locate a specific entry based on the information entered.

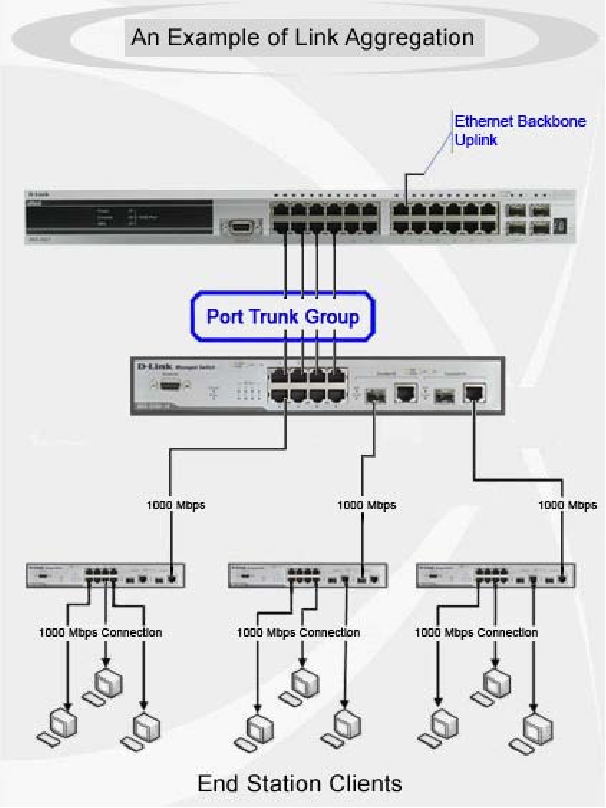
Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. The Switch supports up to 32 port trunk groups with two to eight ports in each group. A potential bit rate of 8000 Mbps can be achieved.



4-35 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of 2 to 8 links (ports). The (optional) Gigabit ports can only belong to a single link aggregation group.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

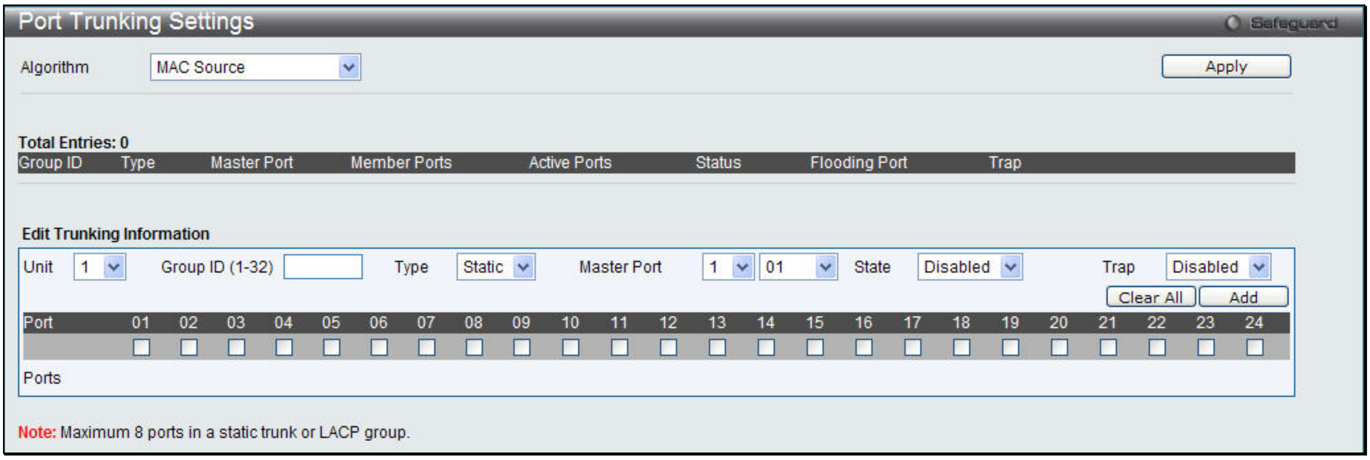
The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

Port Trunking Settings

On this page the user can configure the port trunk settings for the switch.

To view the following window, click **L2 Features > Link Aggregation > Port Trunking Settings**, as show below:



Algorithm: MAC Source

Total Entries: 0

Group ID	Type	Master Port	Member Ports	Active Ports	Status	Flooding Port	Trap

Edit Trunking Information

Unit: 1 Group ID (1-32): Type: Static Master Port: 1 01 State: Disabled Trap: Disabled

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Ports																								

Note: Maximum 8 ports in a static trunk or LACP group.

Figure 4-36 Port Trunking Settings window

The fields that can be configured are described below:

Parameter	Description
Algorithm	This is the traffic hash algorithm among the ports of the link aggregation group. Options to choose from are MAC Source Dest, IP Source Dest and Lay4 Source Dest.
Unit	Select the unit you want to configure.
Group ID (1-32)	Select an ID number for the group, between *1* and *32.*
Type	This drop-down menu allows users to select between *Static* and *LACP* (Link Aggregation Control Protocol). *LACP* allows for the automatic detection of links in a Port Trunking Group.
Master Port	Choose the Master Port for the trunk group using the drop-down menu.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Trap	Use the drop-down menu to enable or disable Link Up and Link Down notifications for this link aggregation group.
Member Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Active Ports	Shows the ports that are currently forwarding packets.

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to clear out all the information entered.

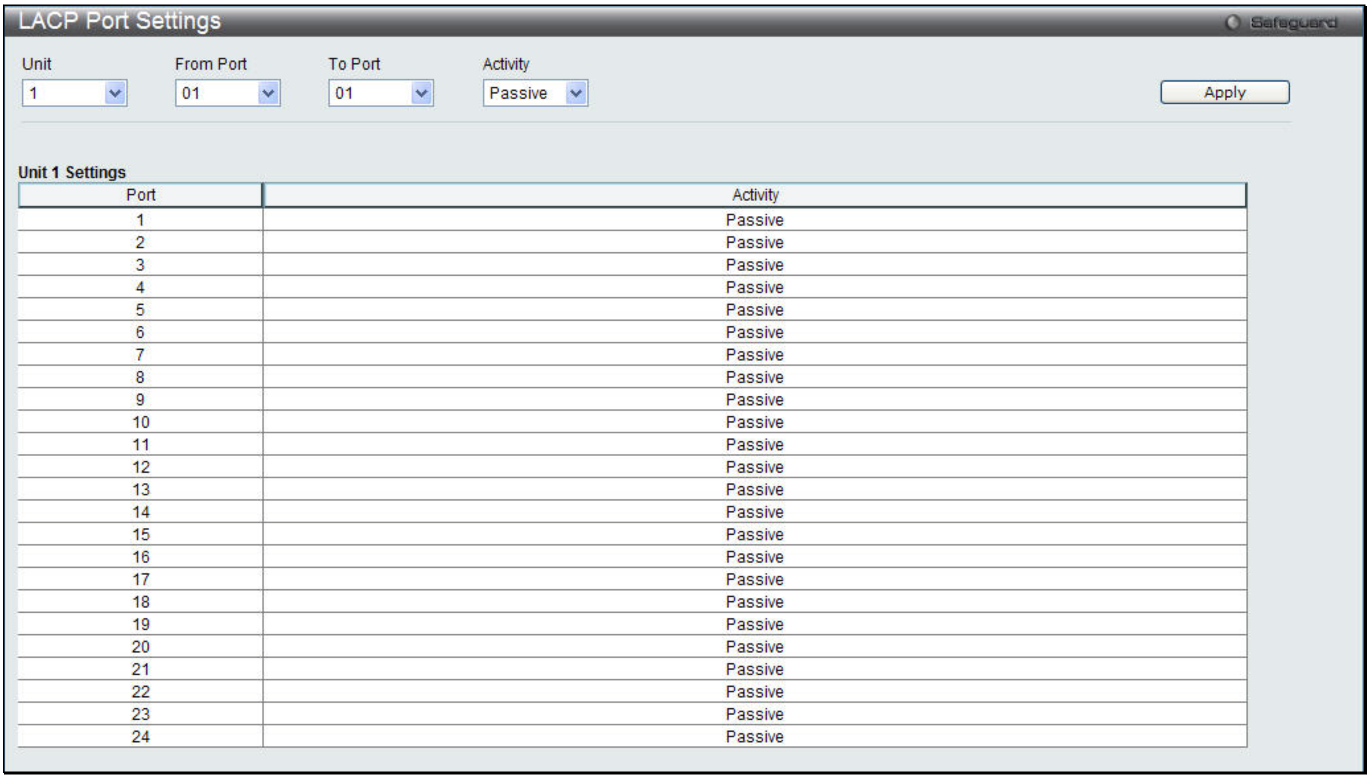
Click the **Add** button to add a new entry based on the information entered.

NOTE: The maximum number of ports that can be configured in one Static Trunk or LACP Group are **8 ports**.

LACP Port Settings

In conjunction with the Trunking window, users can create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

To view the following window, click **L2 Features > Link Aggregation > LACP Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
Activity: Passive

Unit 1 Settings

Port	Activity
1	Passive
2	Passive
3	Passive
4	Passive
5	Passive
6	Passive
7	Passive
8	Passive
9	Passive
10	Passive
11	Passive
12	Passive
13	Passive
14	Passive
15	Passive
16	Passive
17	Passive
18	Passive
19	Passive
20	Passive
21	Passive
22	Passive
23	Passive
24	Passive

Figure 4-37 LACP Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	A consecutive group of ports may be configured starting with the selected port.
Activity	*Active* - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. *Passive* - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).

Click the **Apply** button to accept the changes made.

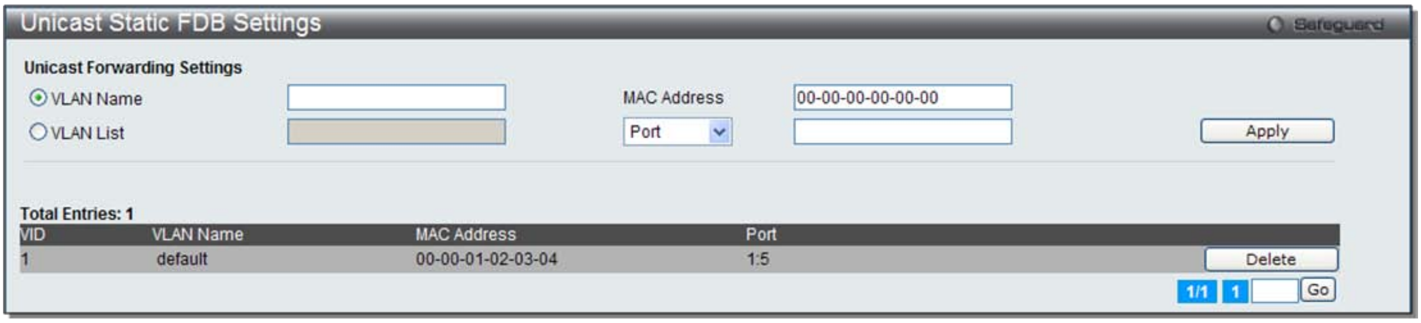
FDB

Static FDB Settings

Unicast Static FDB Settings

Users can set up static unicast forwarding on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB Settings > Unicast Static FDB Settings**, as show below:



● VLAN Name

○ VLAN List

MAC Address: 00-00-00-00-00-00

Port

Total Entries: 1

VID	VLAN Name	MAC Address	Port
1	default	00-00-01-02-03-04	1:5

1/1 1

Figure 4-38 Unicast Static FDB Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN name of the VLAN on which the associated unicast MAC address resides.
VLAN List	Click the radio button and enter a list of VLAN on which the associated unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Port/Drop	Allows the selection of the port number on which the MAC address entered above resides This option could also drop the MAC address from the unicast static FDB. When selecting *Port*, enter the port number in the field. The format can be "unit ID:port number" (e.g. 1:5) or "port number" (e.g. 5). When only entering port number, the default unit ID is 1.

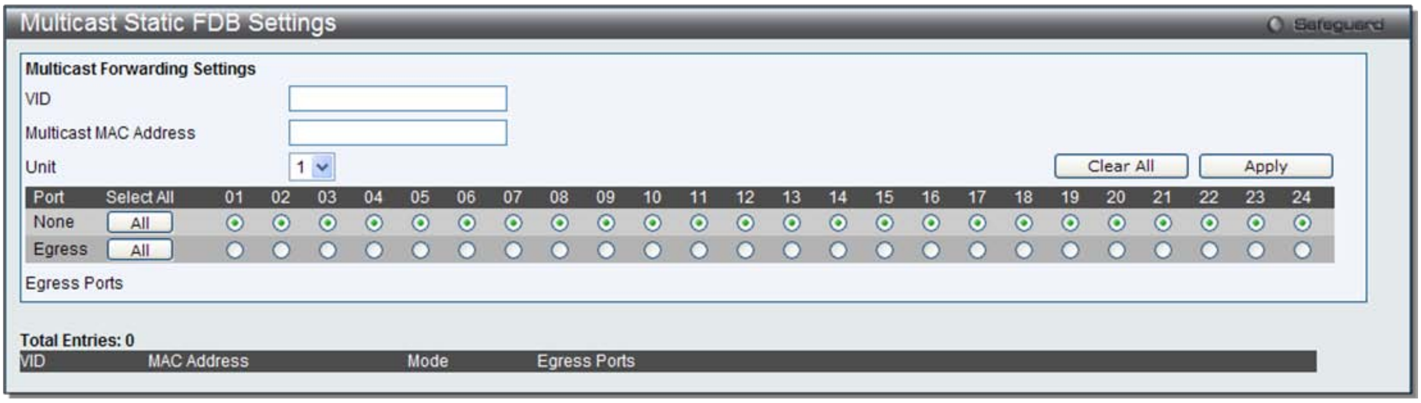
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Multicast Static FDB Settings

Users can set up static multicast forwarding on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB Settings > Multicast Static FDB Settings**, as show below:



Unit: 1

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Egress	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Total Entries: 0

VID	MAC Address	Mode	Egress Ports

Figure 4-39 Multicast Static FDB Settings window

The fields that can be configured are described below:

Parameter	Description
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The static destination MAC address of the multicast packets. This must be a multicast MAC address.
Unit	Select the unit you want to configure.
Port	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are: *None* - No restrictions on the port dynamically joining the multicast group. When *None* is chosen, the port will not be a member of the Static Multicast Group. Click the **All** button to select all the ports. *Egress* - The port is a static member of the multicast group. Click the **All** button to select all the ports.

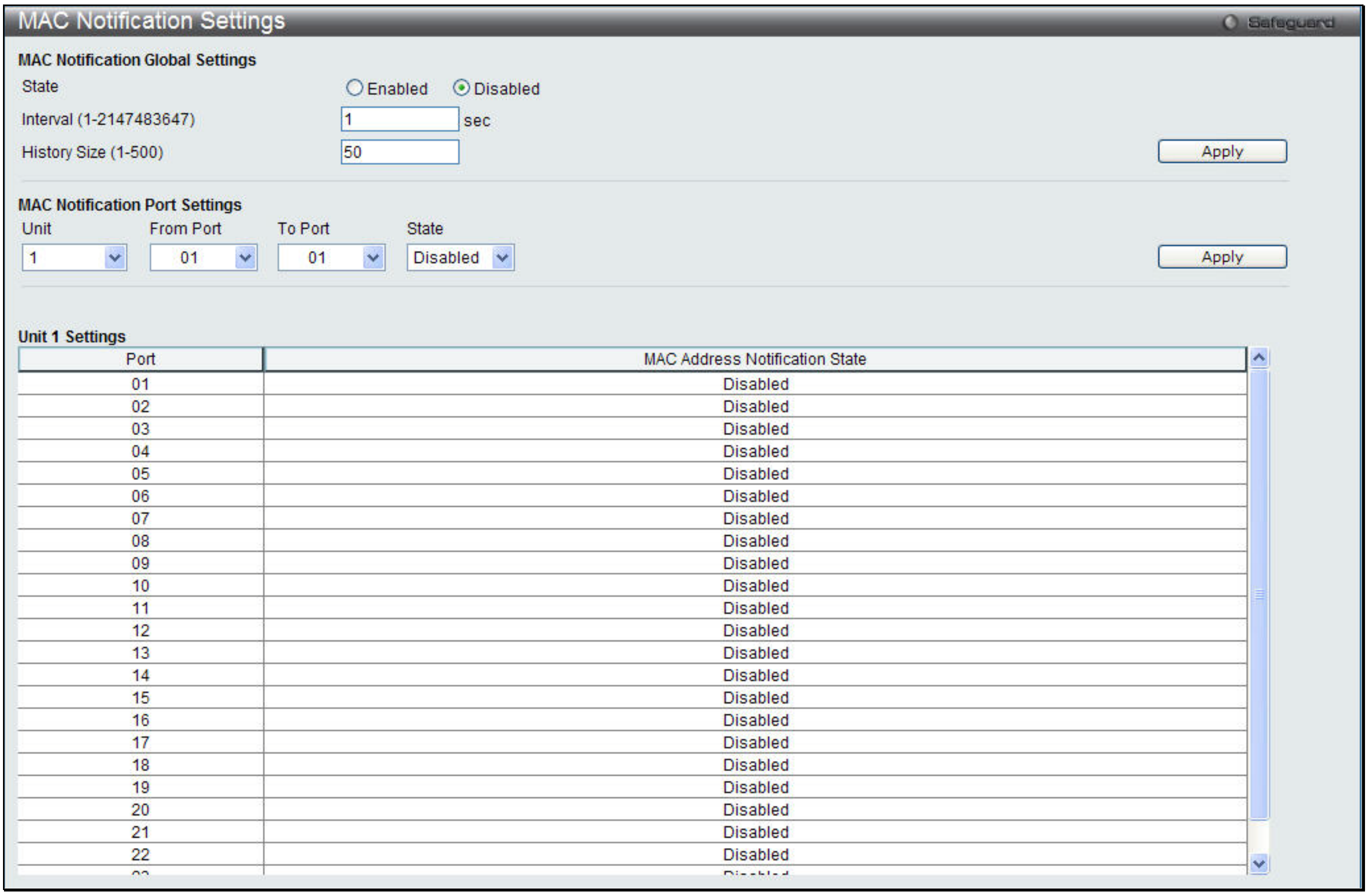
Click the **Clear All** button to clear out all the information entered.

Click the **Apply** button to accept the changes made.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database. This window allows you to globally set MAC notification on the Switch. Users can set MAC notification for individual ports on the Switch.

To view the following window, click **L2 Features > FDB > MAC Notification Settings**, as show below:



MAC Notification Global Settings

State ○ Enabled ● Disabled

Interval (1-2147483647) 1 sec

History Size (1-500) 50

MAC Notification Port Settings

Unit	From Port	To Port	State
1	01	01	Disabled

Unit 1 Settings

Port	MAC Address Notification State
01	Disabled
02	Disabled
03	Disabled
04	Disabled
05	Disabled
06	Disabled
07	Disabled
08	Disabled
09	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled

Figure 4-40 MAC Notification Settings window

The fields that can be configured are described below:

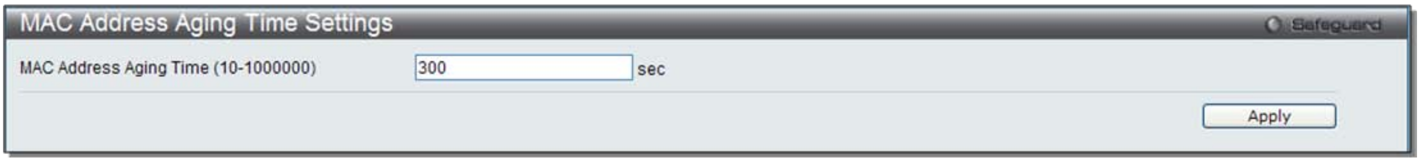
Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (1-2147483647)	The time in seconds between notifications. Value range to use is *1* to *2147483647*.
History Size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.
Unit	Select the unit you want to configure.
From Port / To Port	Select the starting and ending ports for MAC notification.
State	Enable MAC Notification for the ports selected using the drop-down menu.

Click the **Apply** button to accept the changes made for each individual section.

MAC Address Aging Time Settings

Users can configure the MAC Address aging time on the Switch.

To view the following window, click **L2 Features > FDB > MAC Address Aging Time Settings**, as show below:



MAC Address Aging Time (10-1000000) 300 sec

Figure 4-41 MAC Address Aging Time Settings window

The fields that can be configured are described below:

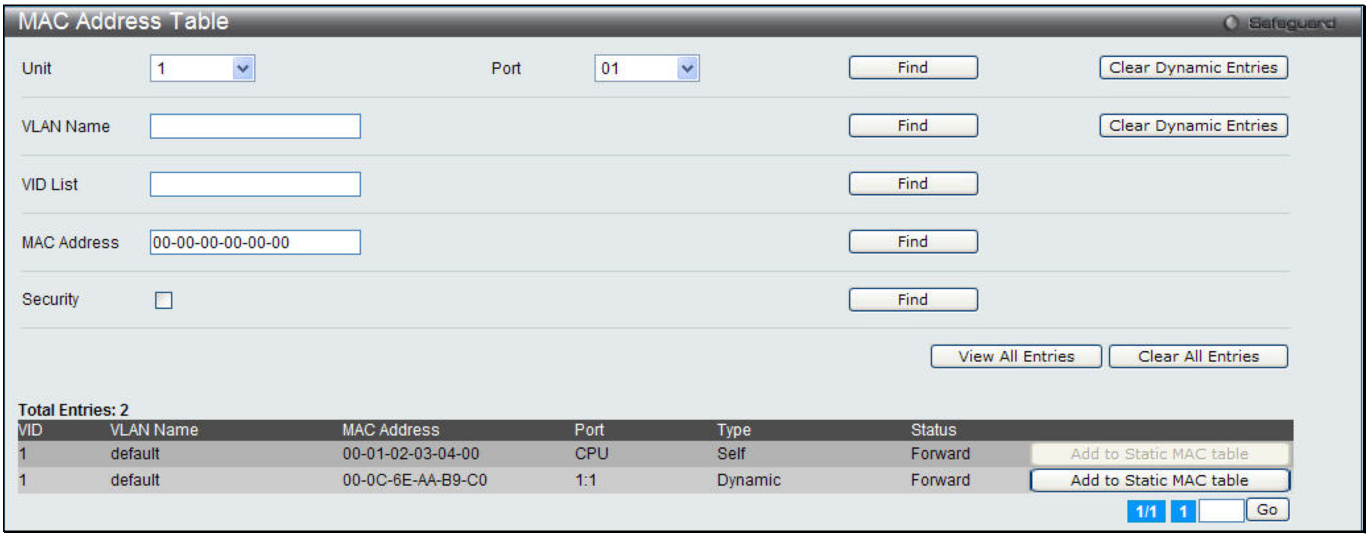
Parameter	Description
MAC Address Aging Time (10-1000000)	This field specify the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this option, type in a different value representing the MAC address' age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *1000000* seconds. The default setting is *300* seconds.

Click the **Apply** button to accept the changes made.

MAC Address Table

This allows the Switch's MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address, VLAN and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as show below:



Unit 1
Port 01
VLAN Name
VID List
MAC Address 00-00-00-00-00-00
Security ☐

Total Entries: 2

VID	VLAN Name	MAC Address	Port	Type	Status
1	default	00-01-02-03-04-00	CPU	Self	Forward
1	default	00-0C-6E-AA-B9-C0	1:1	Dynamic	Forward

Figure 4-42 MAC Address Table window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	The port to which the MAC address below corresponds.
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
VID List	Enter a list of VLAN IDs for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Security	Tick the check box to display the FDB entries that are created by the security module.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Dynamic Entries** button to delete all dynamic entries of the address table.

Click the **View All Entries** button to display all the existing entries.

Click the **Clear All Entries** button to remove all the entries listed in the table.

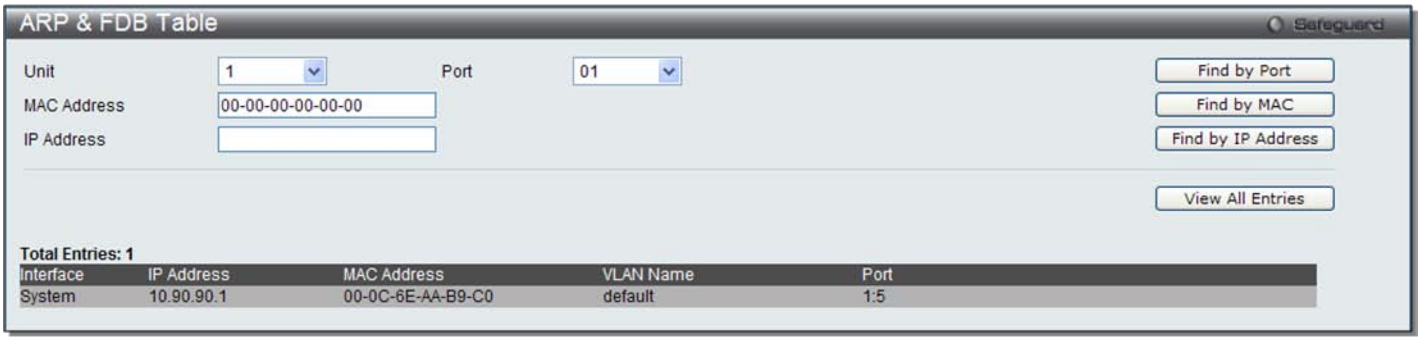
Click the **Add to Static MAC table** button to add the specific entry to the Static MAC table.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ARP & FDB Table

On this page the user can find the ARP and FDB table parameters.

To view the following window, click **L2 Features > FDB > ARP & FDB Table**, as show below:

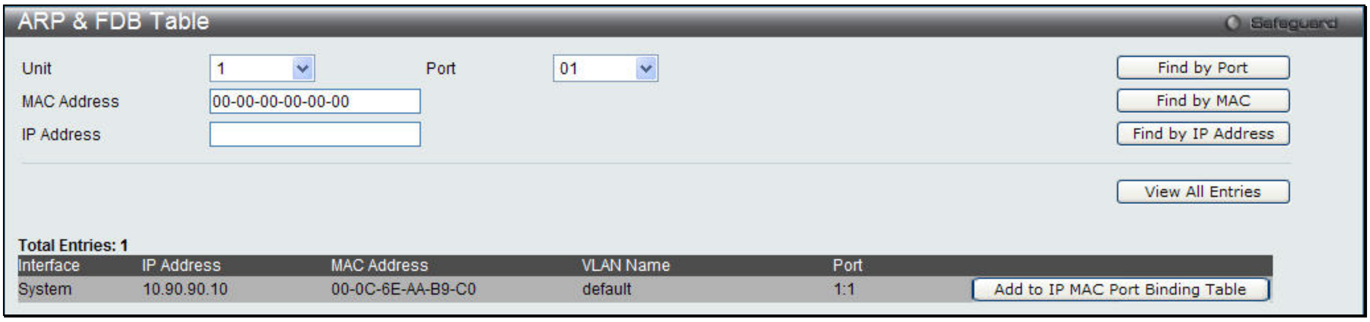


Unit: 1
Port: 01
MAC Address: 00-00-00-00-00-00
IP Address:

Total Entries: 1

Interface	IP Address	MAC Address	VLAN Name	Port
System	10.90.90.1	00-0C-6E-AA-B9-C0	default	1:5

Figure 4-43 ARP & FDB Table window (SI Mode Only)



Unit: 1
Port: 01
MAC Address: 00-00-00-00-00-00
IP Address:

Total Entries: 1

Interface	IP Address	MAC Address	VLAN Name	Port	
System	10.90.90.10	00-0C-6E-AA-B9-C0	default	1:1	Add to IP MAC Port Binding Table

Figure 4-44 ARP & FDB Table window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Select the port number to use for this configuration.
MAC Address	Enter the MAC address to use for this configuration.
IP Address	Enter the IP address the use for this configuration.

Click the **Find by Port** button to locate a specific entry based on the port number selected.

Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.

Click the **Find by IP Address** button to locate a specific entry based on the IP address entered.

Click the **View All Entries** button to display all the existing entries.

Click the **Add to IP MAC Port Binding Table** to add the specific entry to the IMPB Entry Settings window. **(EI Mode Only)**

L2 Multicast Control

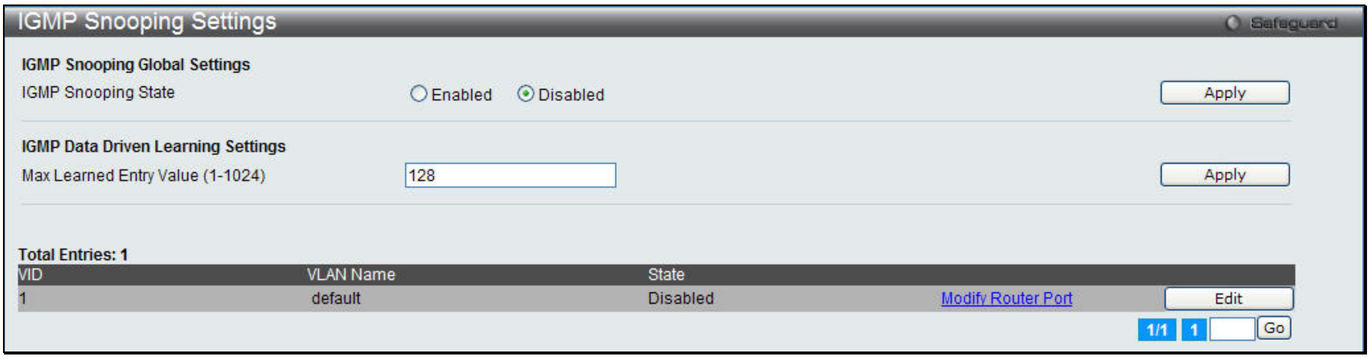
IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP Global Settings at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as show below:



IGMP Snooping Global Settings

IGMP Snooping State ○ Enabled ● Disabled

IGMP Data Driven Learning Settings

Max Learned Entry Value (1-1024): 128

Total Entries: 1

VID	VLAN Name	State		
1	default	Disabled	Modify Router Port	Edit

Figure 4-45 IGMP Snooping Settings window

The fields that can be configured are described below:

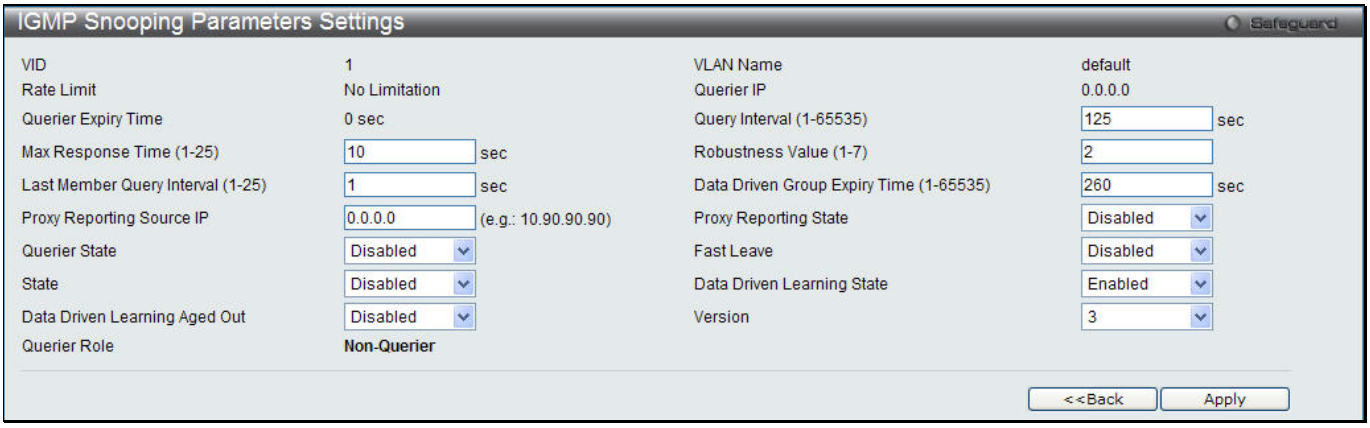
Parameter	Description
IGMP Snooping State	Click to enable or disable the IGMP Snooping state.
Max Learning Entry Value (1-1024)	Enter the maximum learning entry value.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to configure the IGMP Snooping Parameters Settings.

Click the Modify Router Port link to configure the IGMP Snooping Router Port Settings.

After clicking the **Edit** button, the following page will appear:



VID	1	VLAN Name	default
Rate Limit	No Limitation	Querier IP	0.0.0.0
Querier Expiry Time	0 sec	Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec	Robustness Value (1-7)	2
Last Member Query Interval (1-25)	1 sec	Data Driven Group Expiry Time (1-65535)	260 sec
Proxy Reporting Source IP	0.0.0.0 (e.g.: 10.90.90.90)	Proxy Reporting State	Disabled
Querier State	Disabled	Fast Leave	Disabled
State	Disabled	Data Driven Learning State	Enabled
Data Driven Learning Aged Out	Disabled	Version	3
Querier Role	Non-Querier		

Figure 4-46 IGMP Snooping Parameters Settings window

The fields that can be configured are described below:

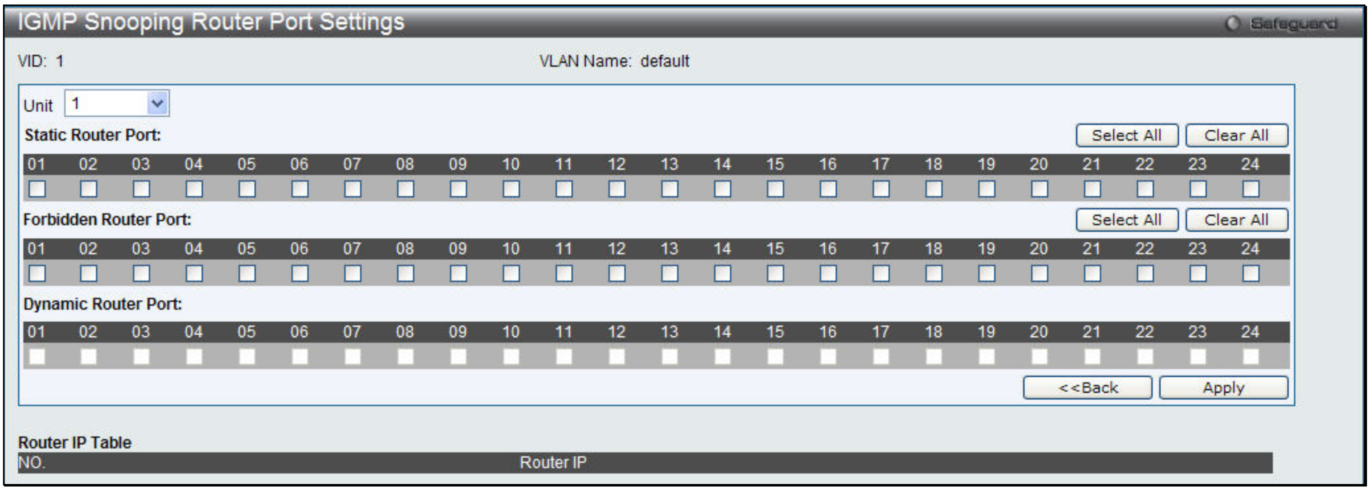
Parameter	Description
Query Interval (1-65535)	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds..
Max Response Time (1-25)	Specify the maximum time in seconds to wait for reports from members. The default setting is 10 seconds.

Robustness Value (1-7)	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness value is used in calculating the following IGMP message intervals: By default, the robustness variable is set to 2.
Last Member Query Interval (1-25)	Specify the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.
Data Drive Group Expiry Time (1-65535)	Specify the data driven group lifetime in seconds.
Proxy Reporting Source IP	Enter the source IP of proxy reporting integrated report.
Proxy Reporting State	Use the drop-down menu to enable or disable the proxy reporting. If enabled, multiple IGMP reports or leave for a specific (S, G) will be integrated into one report only before sending to the router port.
Querier State	Specify to enable or disable the querier state.
Fast Leave	Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
State	If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. **NOTE:** that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.
Data Driven Learning State	Specify to enable or disable the data driven learning state.
Data Drive Learning Aged Out	Specify to enable or disable the data drive learning aged out option.
Version	Specify the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the Modify Router Port link, the following page will appear:


IGMP Snooping Router Port Settings
Safeguard
Static Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Forbidden Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply
Router IP Table
NO.
Router IP

VID: 1

VLAN Name: default

Unit 1

Figure 4-47 IGMP Snooping Router Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Static Router Port	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port	Displays router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

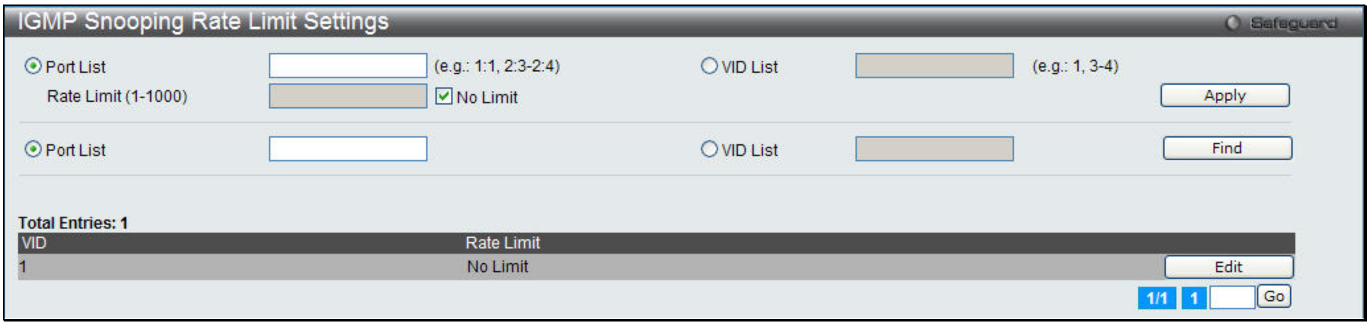
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

IGMP Snooping Rate Limit Settings

On this page the user can configure the IGMP snooping rate limit parameters.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Rate Limit Settings**, as show below:



Total Entries: 1

VID	Rate Limit
1	No Limit

Figure 4-48 IGMP Snooping Rate Limit Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Click the radio button and enter the port list used for this configuration.
VID List	Click the radio button and enter the VID list used for this configuration.
Rate Limit (1-1000)	Enter the IGMP snooping rate limit used. Tick the **No Limit** check box to ignore the rate limit.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

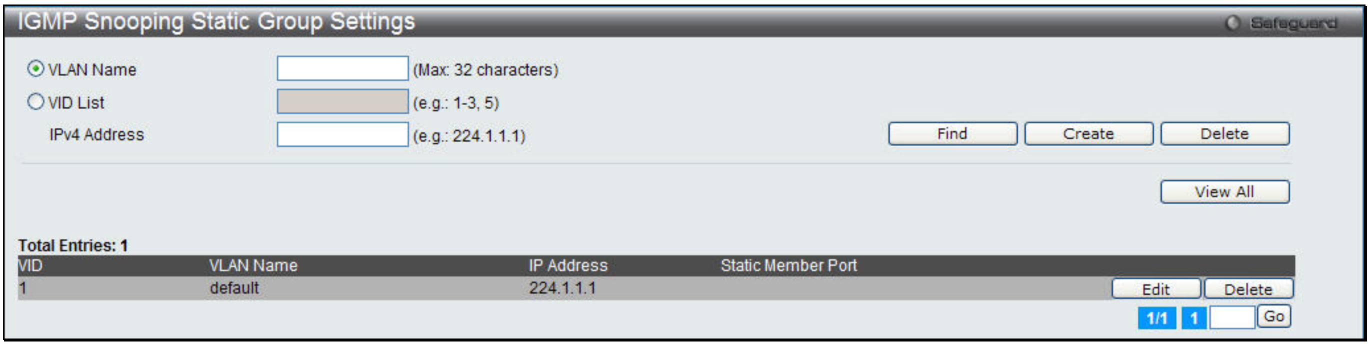
Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Snooping Static Group Settings

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Static Group Settings**, as show below:



● VLAN Name (Max: 32 characters)
○ VID List (e.g.: 1-3, 5)
IPv4 Address (e.g.: 224.1.1.1)

Total Entries: 1

VID	VLAN Name	IP Address	Static Member Port
1	default	224.1.1.1	

Figure 4-49 IGMP Snooping Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the VLAN name of the multicast group.
VID List	Enter the VID list or of the multicast group.
IPv4 Address	Enter the IPv4 address.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Create** button to add a new entry based on the information entered.

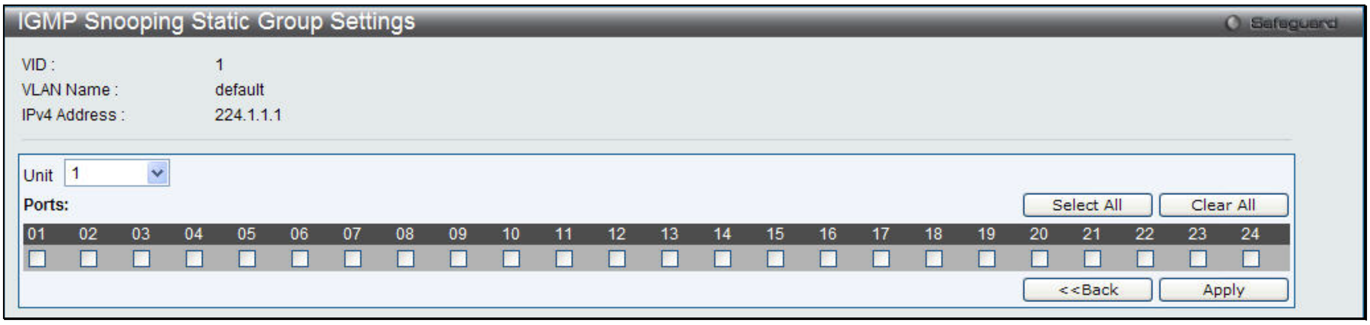
Click the **Delete** button to remove the specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following page will appear:



VID : 1
VLAN Name : default
IPv4 Address : 224.1.1.1

Unit 1

Ports:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 4-50 IGMP Snooping Static Group Settings window

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

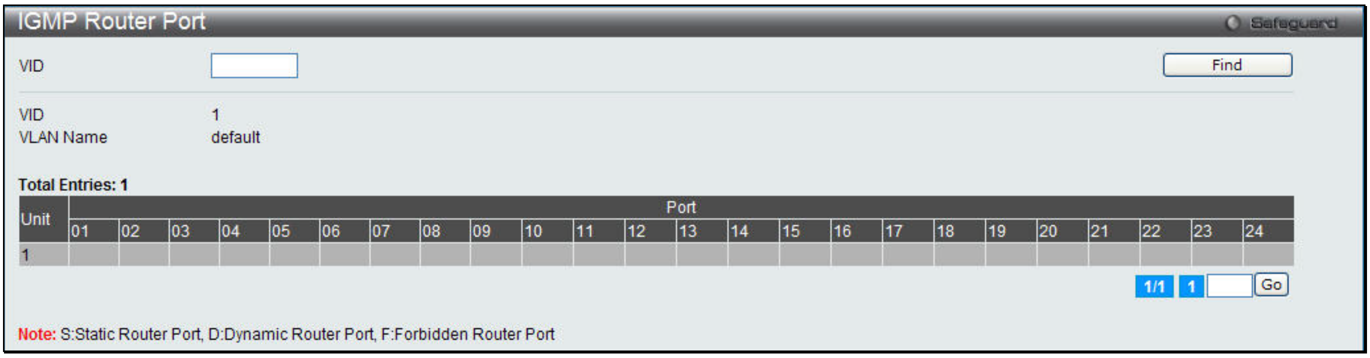
Click the **<<Back** button to discard the changes made and return to the previous page.

IGMP Router Port

Users can display which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S.

A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Router Port**, as show below:


IGMP Router Port
Safeguard
VID
Find
1/1
1
Go

VID 1

VLAN Name default

Total Entries: 1

Unit	Port 01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								

Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

Figure 4-51 IGMP Router Port window

Enter a VID (VLAN ID) in the field at the top of the window.

Click the **Find** button to locate a specific entry based on the information entered.

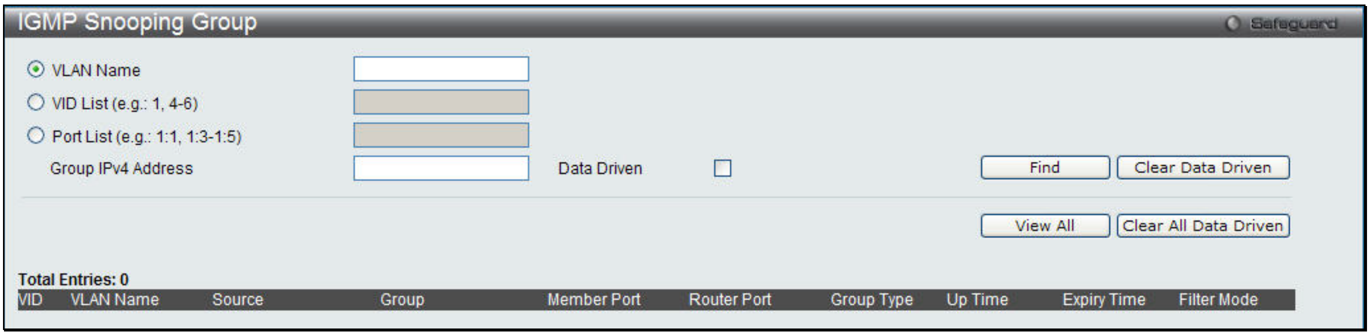
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE: The abbreviations used on this page are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

IGMP Snooping Group

Users can view the Switch's IGMP Snooping Group Table. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group**, as show below:


IGMP Snooping Group
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
○ Port List (e.g.: 1:1, 1:3-1:5)
Group IPv4 Address
Data Driven ☐
Find
Clear Data Driven
View All
Clear All Data Driven

Total Entries: 0

VID	VLAN Name	Source	Group	Member Port	Router Port	Group Type	Up Time	Expiry Time	Filter Mode

Figure 4-52 IGMP Snooping Group window

The user may search the IGMP Snooping Group Table by either *VLAN Name* or *VID List* by entering it in the top left hand corner and clicking **Find**.

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.
Port List	Specify the port number(s) used to find a multicast group.
Group IPv4 Address	Enter the IPv4 address.

Data Driven	If selected, only data driven groups will be displayed.

Click the **Clear Data Driven** button to delete the specific IGMP snooping group which is learned by the Data Driven feature of the specified VLAN.

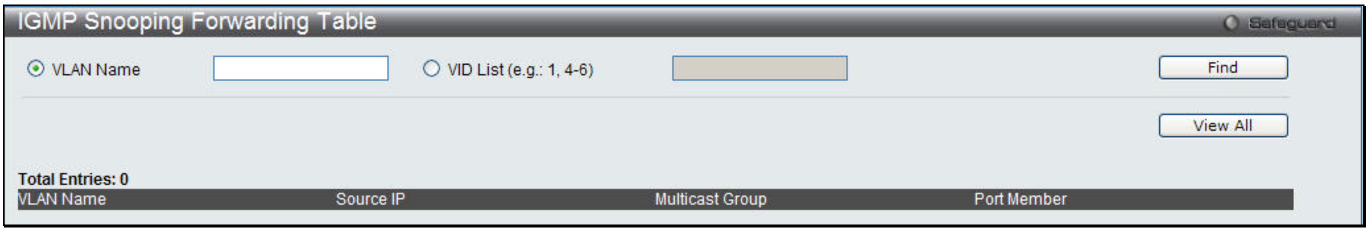
Click the **View All** button to display all the existing entries.

Click the **Clear All Data Driven** button to delete all IGMP snooping groups which is learned by the Data Driven feature of specified VLANs.

IGMP Snooping Forwarding Table

This page displays the switch's current IGMP snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The IGMP snooping further restricts the forwarding ports.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Forwarding Table**, as show below:


IGMP Snooping Forwarding Table
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
Find
View All
VLAN Name
Source IP
Multicast Group
Port Member

Total Entries: 0

Figure 4-53 IGMP Snooping Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
VID List	The VLAN ID list of the multicast group.

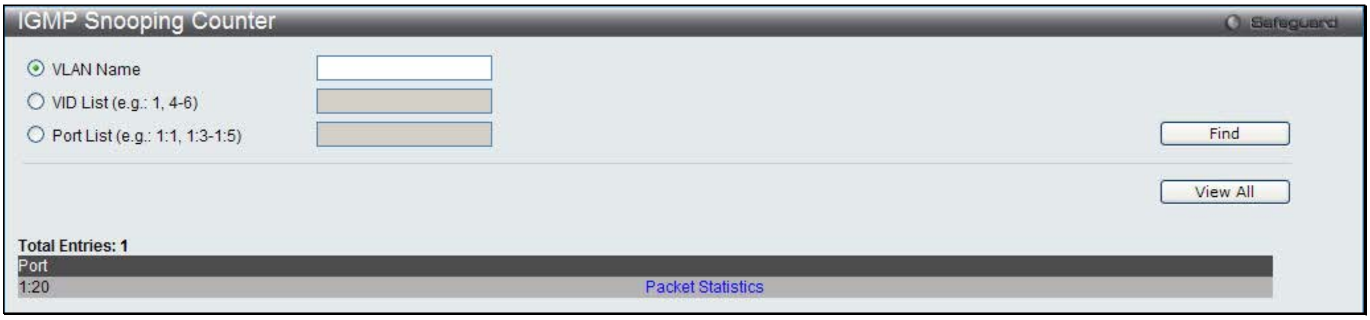
Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

IGMP Snooping Counter

Users can view the switch's IGMP Snooping counter table.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Counter**, as show below:


IGMP Snooping Counter
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
○ Port List (e.g.: 1:1, 1:3-1:5)
Find
View All
Port

Total Entries: 1

1:20 Packet Statistics

Figure 4-54 IGMP Snooping Counter window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.

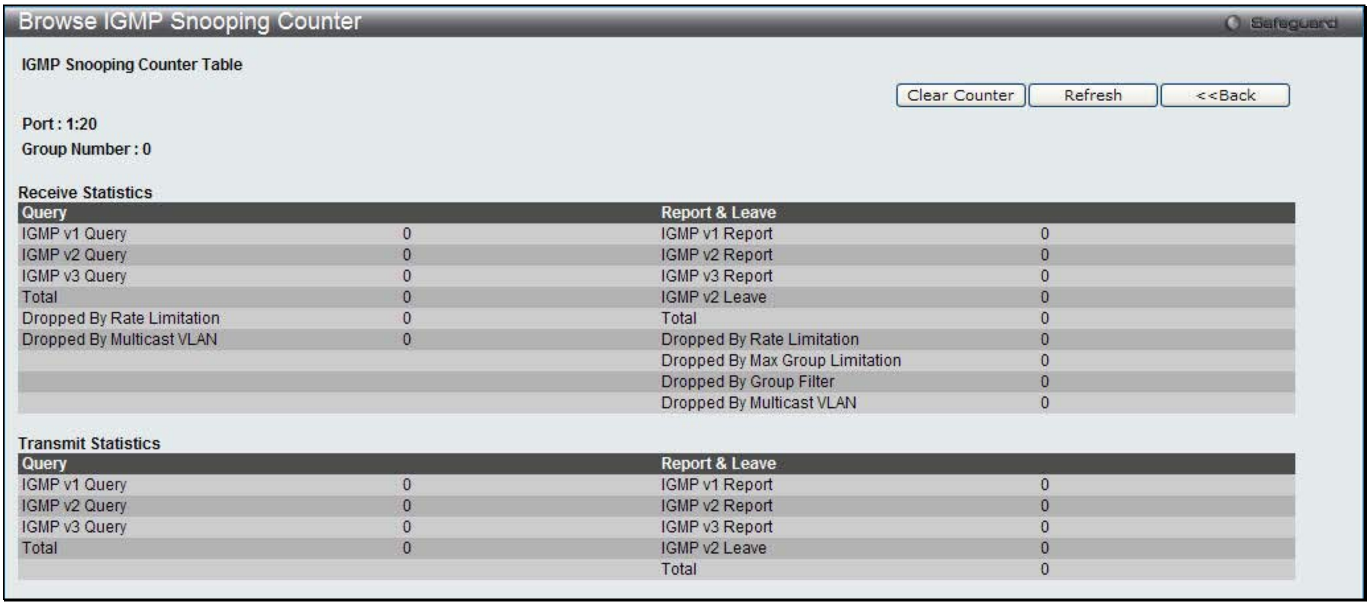
VID List	The VLAN ID list of the multicast group.
Port List	The *Port List* of the multicast group.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the Packet Statistics link to view the IGMP Snooping Counter Table.

After clicking the Packet Statistics link, the following page will appear:



IGMP Snooping Counter Table

Port : 1:20

Group Number : 0

Receive Statistics

Query		Report & Leave	
IGMP v1 Query	0	IGMP v1 Report	0
IGMP v2 Query	0	IGMP v2 Report	0
IGMP v3 Query	0	IGMP v3 Report	0
Total	0	IGMP v2 Leave	0
Dropped By Rate Limitation	0	Total	0
Dropped By Multicast VLAN	0	Dropped By Rate Limitation	0
		Dropped By Max Group Limitation	0
		Dropped By Group Filter	0
		Dropped By Multicast VLAN	0

Transmit Statistics

Query		Report & Leave	
IGMP v1 Query	0	IGMP v1 Report	0
IGMP v2 Query	0	IGMP v2 Report	0
IGMP v3 Query	0	IGMP v3 Report	0
Total	0	IGMP v2 Leave	0
		Total	0

Figure 4-55 Browse IGMP Snooping Counter window

Click the **Clear Counter** button to clear all the information displayed in the fields.

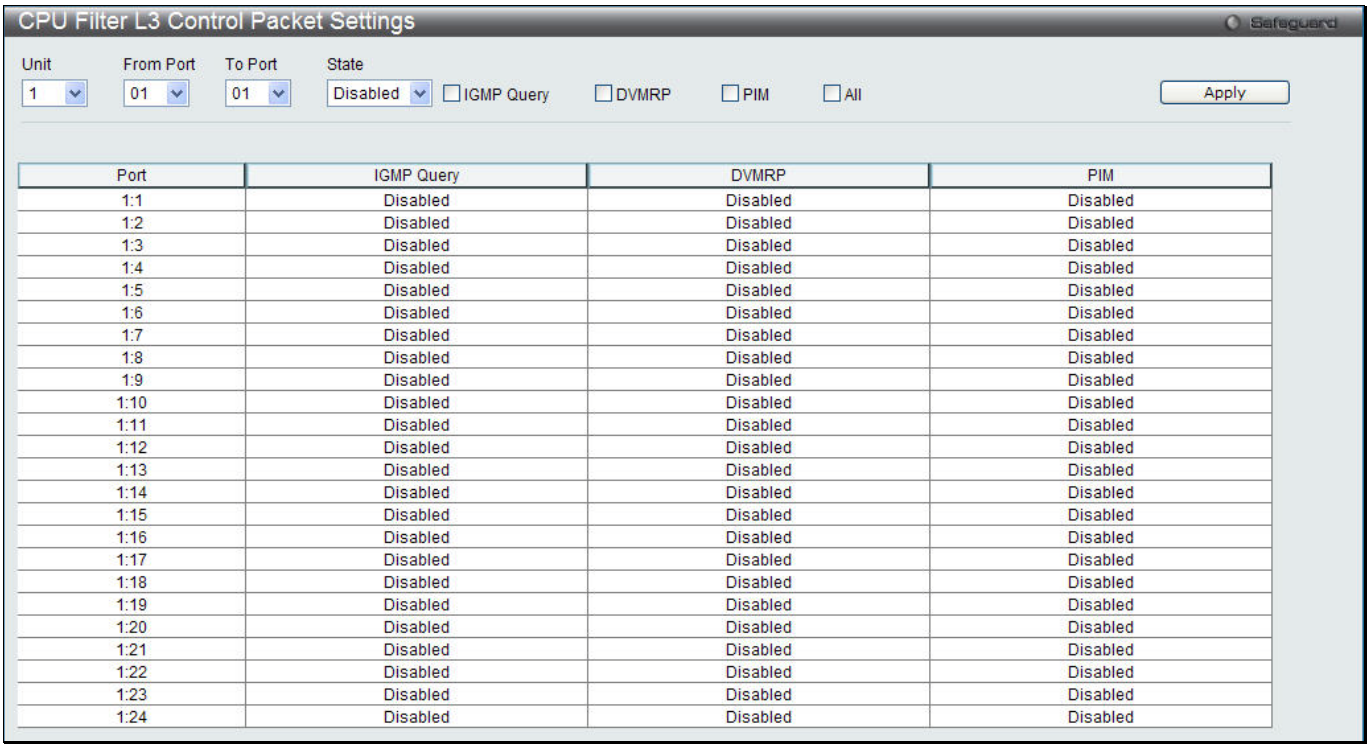
Click the **Refresh** button to refresh the display table so that new information will appear.

Click the **<<Back** button to return to the previous page.

CPU Filter L3 Control Packet Settings

This window is used to discard and display Layer 3 control packets sent to the CPU from specific ports.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > CPU Filter L3 control Packet Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
State: Disabled
☐ IGMP Query ☐ DVMRP ☐ PIM ☐ All

Port	IGMP Query	DVMRP	PIM
1:1	Disabled	Disabled	Disabled
1:2	Disabled	Disabled	Disabled
1:3	Disabled	Disabled	Disabled
1:4	Disabled	Disabled	Disabled
1:5	Disabled	Disabled	Disabled
1:6	Disabled	Disabled	Disabled
1:7	Disabled	Disabled	Disabled
1:8	Disabled	Disabled	Disabled
1:9	Disabled	Disabled	Disabled
1:10	Disabled	Disabled	Disabled
1:11	Disabled	Disabled	Disabled
1:12	Disabled	Disabled	Disabled
1:13	Disabled	Disabled	Disabled
1:14	Disabled	Disabled	Disabled
1:15	Disabled	Disabled	Disabled
1:16	Disabled	Disabled	Disabled
1:17	Disabled	Disabled	Disabled
1:18	Disabled	Disabled	Disabled
1:19	Disabled	Disabled	Disabled
1:20	Disabled	Disabled	Disabled
1:21	Disabled	Disabled	Disabled
1:22	Disabled	Disabled	Disabled
1:23	Disabled	Disabled	Disabled
1:24	Disabled	Disabled	Disabled

Figure 4-56 CPU Filter L3 Control Packet Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the a range of ports to be configured.
State	Use the drop-down menu to enable or disable the filtering function
IGMP Query	Tick to enable or disable filtering IGMP Query protocol packets.
DVMRP	Tick to enable or disable filtering DVMRP protocol packets.
PIM	Tick to enable or disable filtering PIM protocol packets.
All	Tick to enable or disable filtering all layer 3 control packets.

Click the **Apply** button to accept the changes made.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

1. **Multicast Listener Query** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report, Version 1** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
4. **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

Data Driven Learning

The Switch allows you to implement data driven learning for MLD snooping groups. If data-driven learning, also known as dynamic IP multicast learning, is enabled for a VLAN, when the Switch receives IP multicast traffic on the VLAN, an MLD snooping group is created. Learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to age out or to age out by a timer.

When the data driven learning State is enabled, the multicast filtering mode for all ports is ignored. This means multicast packets will be flooded.

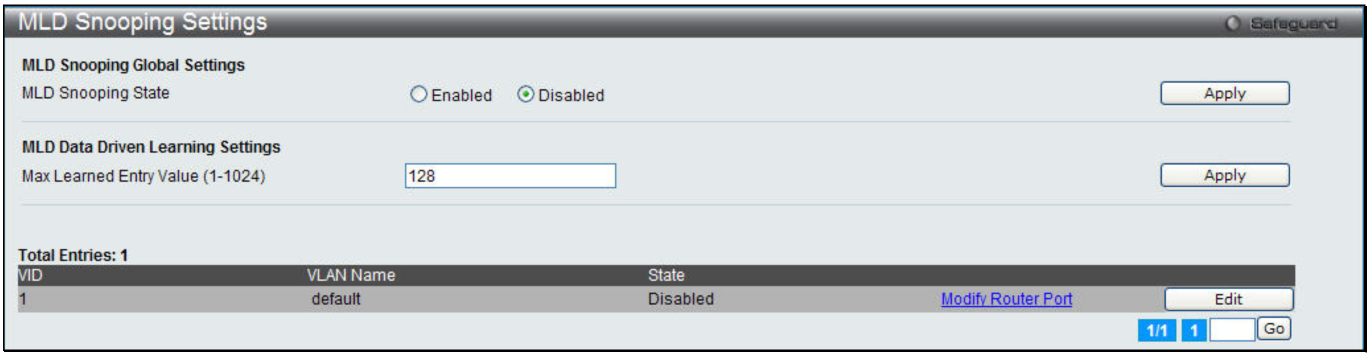
NOTE: If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. In other words, the aging out mechanism will follow the conditions of an ordinary MLD snooping entry.

Data driven learning is useful on a network which has video cameras connected to a Layer 2 switch that is recording and sending IP multicast data. The switch needs to forward IP data to a data centre without dropping or flooding any packets. Since video cameras do not have the capability to run MLD protocols, the IP multicast data will be dropped with the original MLD snooping function.

MLD Snooping Settings

Users can configure the settings for MLD snooping.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings**, as show below:



MLD Snooping Global Settings

MLD Snooping State ○ Enabled ● Disabled

MLD Data Driven Learning Settings

Max Learned Entry Value (1-1024): 128

Total Entries: 1

VID	VLAN Name	State		
1	default	Disabled	Modify Router Port	Edit

Figure 4-57 MLD Snooping Settings window

The fields that can be configured are described below:

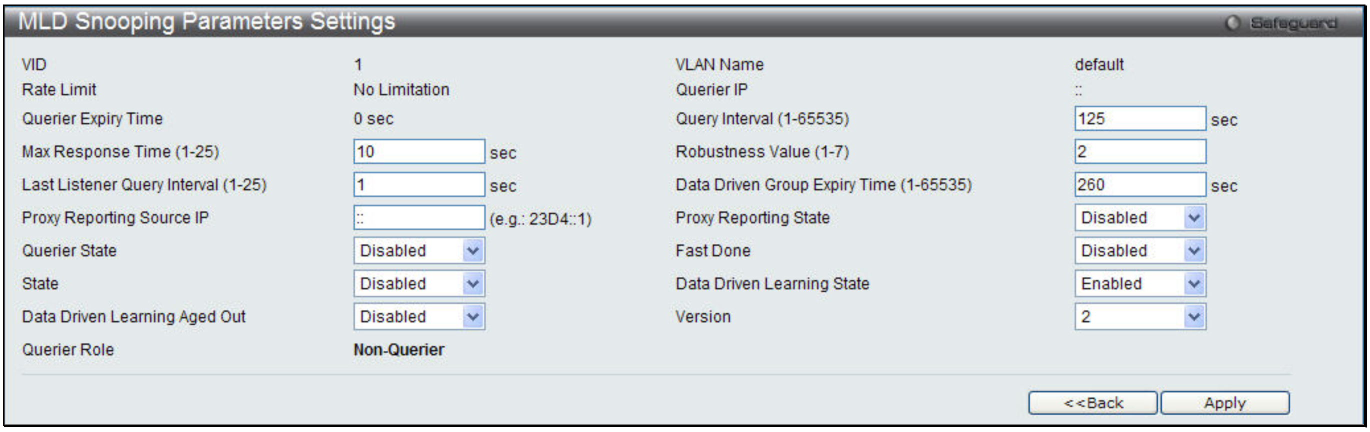
Parameter	Description
MLD Snooping State	Click to enable or disable the MLD snooping state.
Max Learning Entry Value (1-1024)	Enter the maximum learning entry value.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to configure the MLD Snooping Parameters Settings for a specific entry.

Click the Modify Router Port link to configure the MLD Snooping Router Port Settings for a specific entry.

After clicking the **Edit** button, the following page will appear:



MLD Snooping Parameters Settings

VID	1	VLAN Name	default
Rate Limit	No Limitation	Querier IP	::
Querier Expiry Time	0 sec	Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec	Robustness Value (1-7)	2
Last Listener Query Interval (1-25)	1 sec	Data Driven Group Expiry Time (1-65535)	260 sec
Proxy Reporting Source IP	:: (e.g.: 23D4::1)	Proxy Reporting State	Disabled
Querier State	Disabled	Fast Done	Disabled
State	Disabled	Data Driven Learning State	Enabled
Data Driven Learning Aged Out	Disabled	Version	2
Querier Role	Non-Querier		

Figure 4-58 MLD Snooping Parameters Settings window

The fields that can be configured are described below:

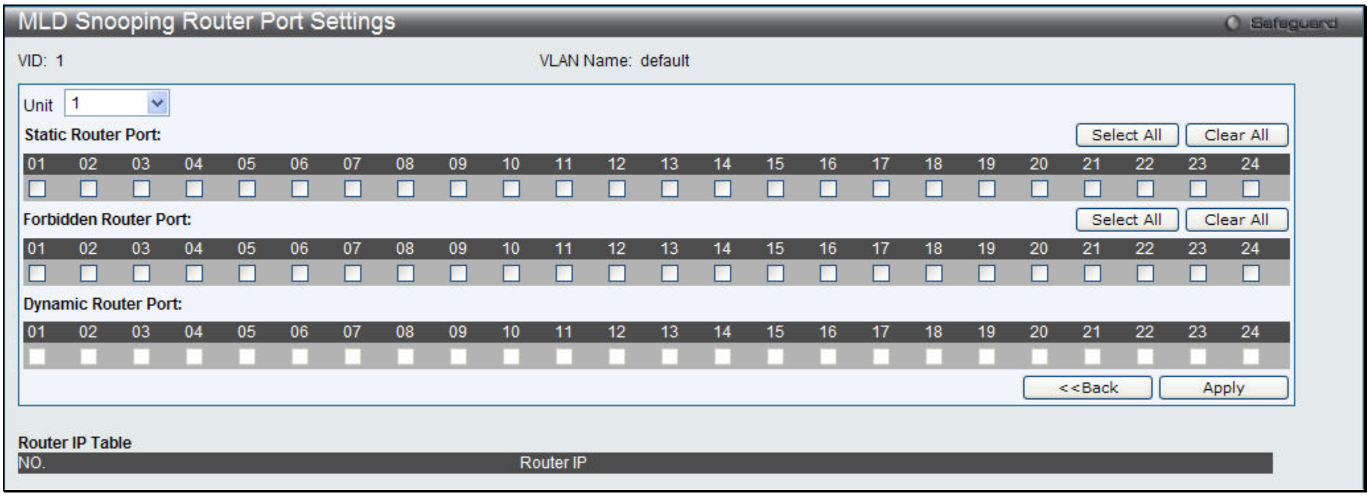
Parameter	Description
Query Interval (1-65535)	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
Max Response Time (1-25)	The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
Robustness Value (1-7)	Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: *Group listener interval* - Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. *Other Querier present interval* - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the Querier. *Last listener query count* - Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be loosely.
Last Listener Query Interval (1-25)	The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
Data Driven Group Expiry Time (1-65535)	Enter the data driven group expiry time value.
Proxy Reporting Source IP	Enter the source IP of proxy reporting integrated report.
Proxy Reporting State	Use the drop-down menu to enable or disable the proxy reporting.

Querier State	This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
Fast Done	Here the user can enable or disable the fast done feature.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is *Disabled* by default.
Data Driven Learning State	Enable or disable data driven learning of MLD snooping groups.
Data Driven Learning Aged Out	Enable or disable the age out function for data driven entries.
Version	Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the Modify Router Port link, the following page will appear:


MLD Snooping Router Port Settings
Safeguard
Static Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Forbidden Router Port:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Dynamic Router Port:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply
Router IP Table
NO.
Router IP

VID: 1

VLAN Name: default

Unit 1

Figure 4-59 MLD Snooping Router Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Static Router Port	This section is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router regardless of the protocol.
Forbidden Router Port	This section is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Dynamic Router Port	Display router ports that have been dynamically configured.
Ports	Select the appropriate ports individually to include them in the Router Port configuration.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

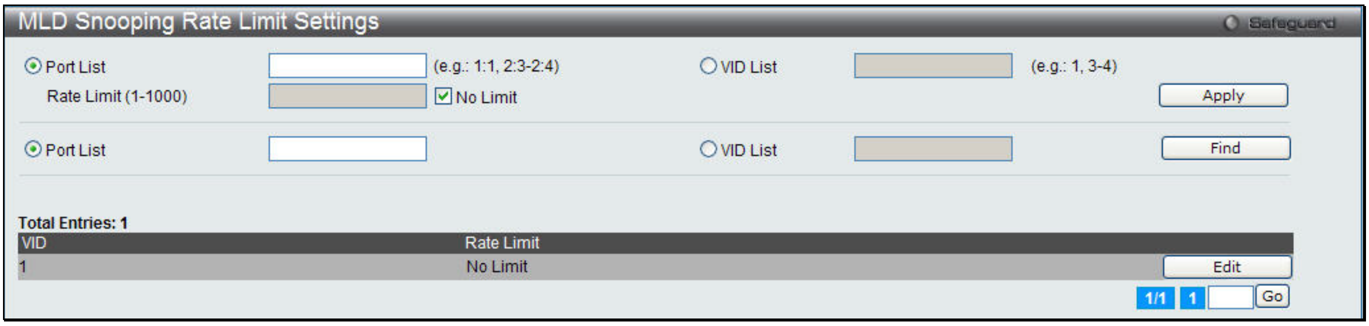
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

MLD Snooping Rate Limit Settings

Users can configure the rate limit of the MLD control packet that the switch can process on a specific port or VLAN in this page.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Rate Limit Settings**, as show below:


MLD Snooping Rate Limit Settings
Safeguard
● Port List
(e.g.: 1:1, 2:3-2:4)
○ VID List
(e.g.: 1, 3-4)
Rate Limit (1-1000)
☑ No Limit
Apply
● Port List
○ VID List
Find
Edit
1/1
1
Go

Total Entries: 1

VID	Rate Limit
1	No Limit

Figure 4-60 MLD Snooping Rate Limit Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter the Port List here.
VID List	Enter the VID List value here.
Rate Limit	Configure the rate limit of MLD control packet that the switch can process on a specific port/VLAN. The rate is specified in packet per second. The packet that exceeds the limited rate will be dropped. Tick the **No Limit** check box to lift the rate limit requirement.

Click the **Apply** button to accept the changes made for each individual section.

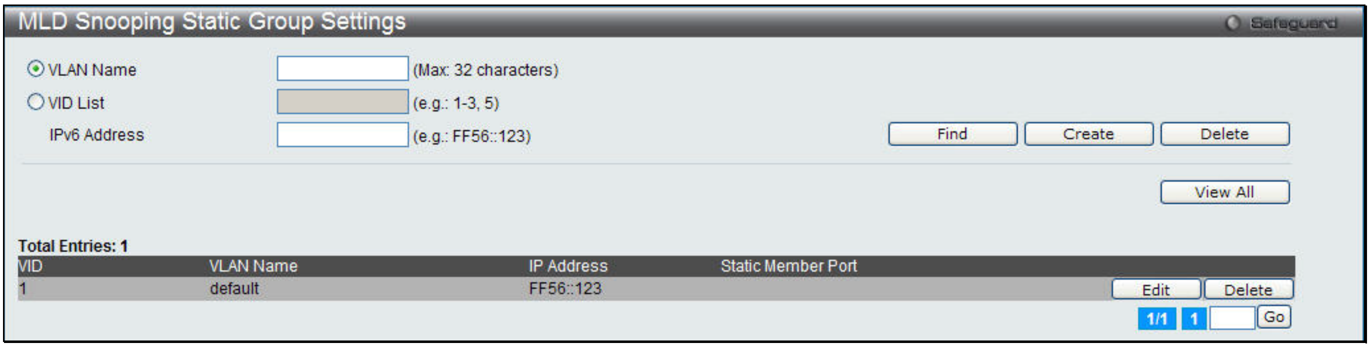
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to re-configure the specific entry.

MLD Snooping Static Group Settings

This page used to configure the MLD snooping multicast group static members.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Static Group Settings**, as show below:


MLD Snooping Static Group Settings
Safeguard
● VLAN Name
(Max: 32 characters)
○ VID List
(e.g.: 1-3, 5)
IPv6 Address
(e.g.: FF56::123)
Find
Create
Delete
View All
Edit
Delete
1/1
1
Go

Total Entries: 1

VID	VLAN Name	IP Address	Static Member Port
1	default	FF56::123	

Figure 4-61 MLD Snooping Static Group Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN on which the static group resides.
VID List	The ID of the VLAN on which the static group resides.

IPv6 Address	Specify the multicast group IPv6 address.

Click the **Find** button to locate a specific entry based on the information entered.

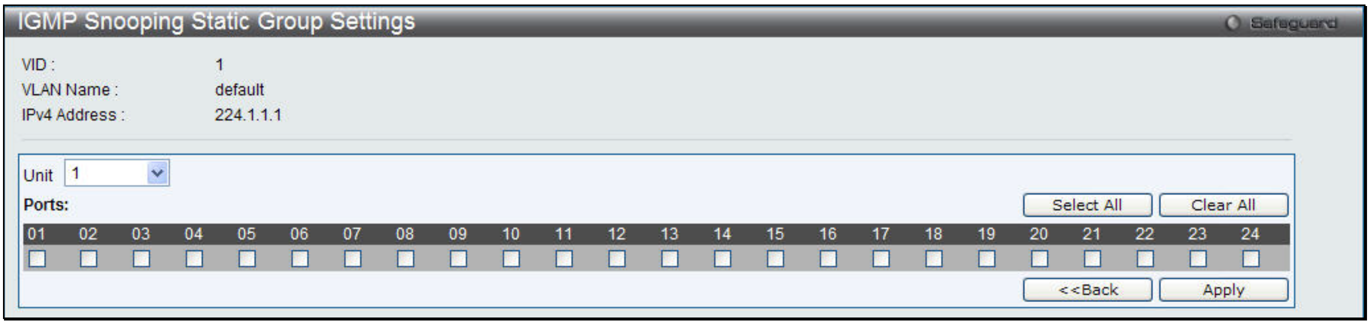
Click the **Create** button to add a static group.

Click the **Delete** button to delete a static group.

Click the **View All** button to display all the existing entries.

Click the **Edit** button to re-configure the specific entry.

After clicking the **Edit** button, the following page will appear:


IGMP Snooping Static Group Settings
Safeguard
Unit
Ports:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
<<Back
Apply

VID : 1
VLAN Name : default
IPv4 Address : 224.1.1.1
Unit 1

Figure 4-62 MLD Snooping Static Group Settings – Edit window

Parameter	Description
Unit	Select the unit you want to configure.
Ports	Tick the check boxes to select the ports to be configured.

Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

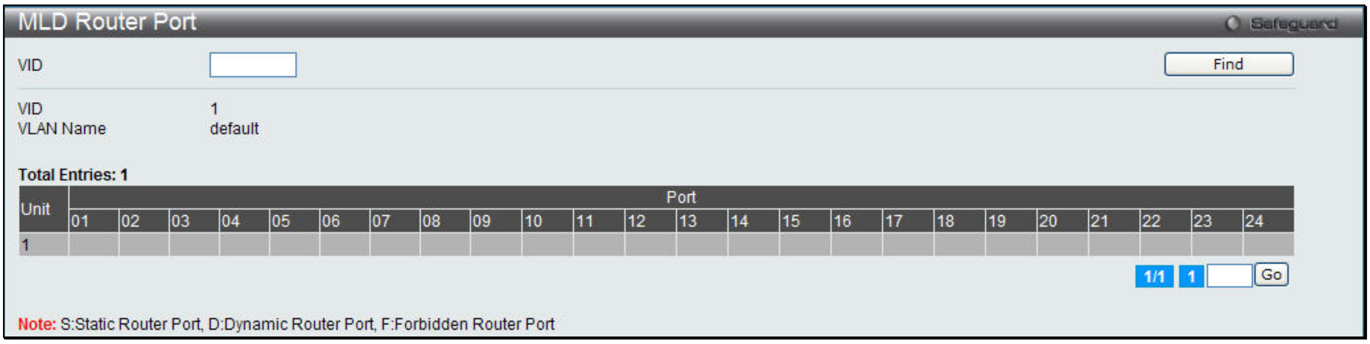
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

MLD Router Port

Users can display which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D, while a Forbidden port is designated by F.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Router Port**, as show below:


MLD Router Port
Safeguard
VID
Find
1/1
1
Go

VID 1
VLAN Name default

Total Entries: 1

Unit	Port																							
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								

Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

Figure 4-63 MLD Router Port window

Parameter	Description
VID	Enter a VLAN ID.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

NOTE: The abbreviations used on this page are **Static Router Port (S)**, **Dynamic Router Port (D)** and **Forbidden Router Port (F)**.

MLD Snooping Group

Users can view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group**, as show below:

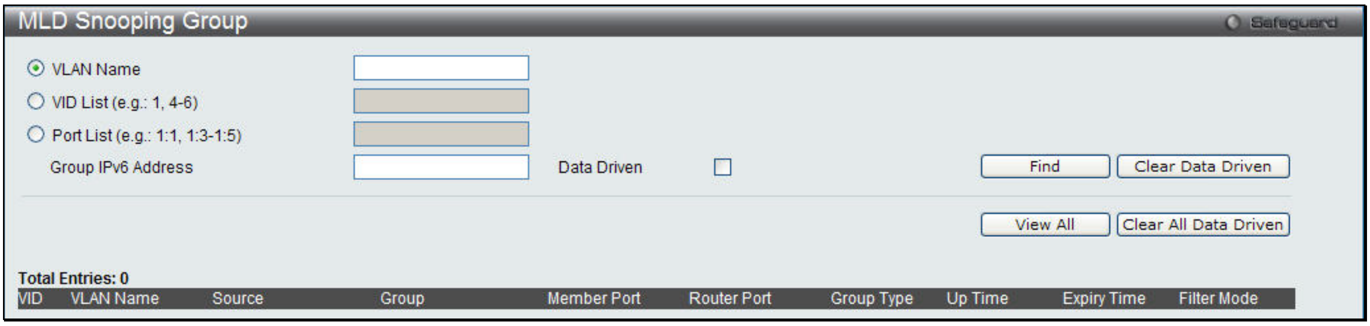

MLD Snooping Group
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
○ Port List (e.g.: 1:1, 1:3-1:5)
Group IPv6 Address
Data Driven ☐
Find
Clear Data Driven
View All
Clear All Data Driven
Total Entries: 0
VID
VLAN Name
Source
Group
Member Port
Router Port
Group Type
Up Time
Expiry Time
Filter Mode

Figure 4-64 MLD Snooping Group window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the radio button and enter the VLAN name of the multicast group.
VID List	Click the radio button and enter a VLAN list of the multicast group.
Port List	Specify the port number(s) used to find a multicast group.
Group IPv6 Address	Enter the group IPv6 address used here. Select the **Data Driven** option to enable the data driven feature for this MLD snooping group.
Data Driven	If Data Drive is selected, only data driven groups will be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Data Driven** button to delete the specific MLD snooping group which is learned by the Data Driven feature of the specified VLAN.

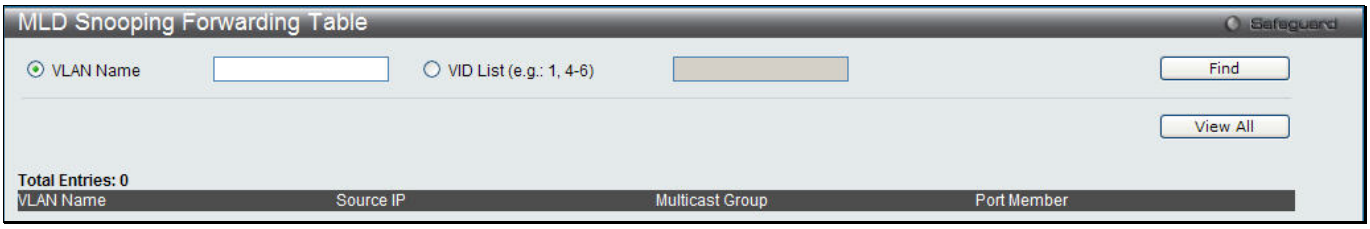
Click the **View All** button to display all the existing entries.

Click the **Clear All Data Driven** button to delete all MLD snooping groups which is learned by the Data Driven feature of specified VLANs.

MLD Snooping Forwarding Table

This page displays the switch's current MLD snooping forwarding table. It provides an easy way for user to check the list of ports that the multicast group comes from and specific sources that it will be forwarded to. The packet comes from the source VLAN. They will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Forwarding Table**, as show below:


MLD Snooping Forwarding Table
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
Find
View All

Total Entries: 0

VLAN Name	Source IP	Multicast Group	Port Member

Figure 4-65 MLD Snooping Forwarding Table window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	The name of the VLAN for which you want to view MLD snooping forwarding table information.
VID List	The ID of the VLAN for which you want to view MLD snooping forwarding table information.

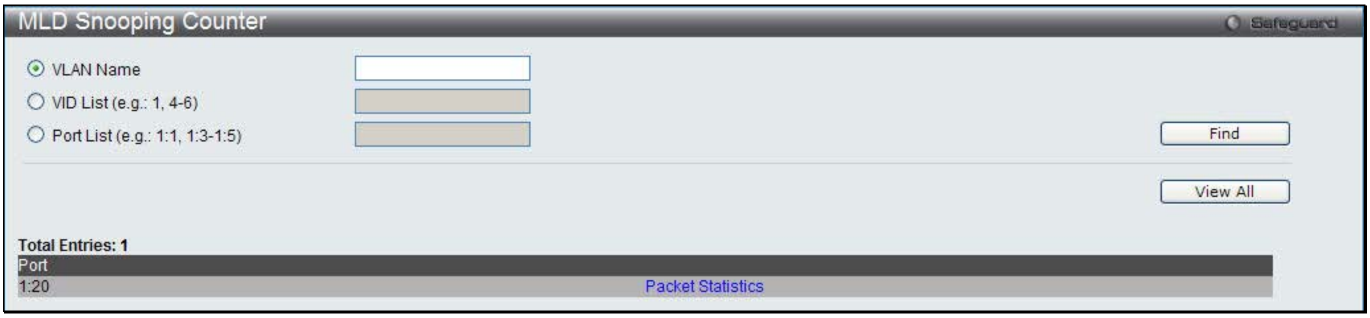
Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

MLD Snooping Counter

This page displays the statistics counter for MLD protocol packets that are received by the switch since MLD Snooping is enabled.

To view the following window, click **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Counter**, as show below:


MLD Snooping Counter
Safeguard
● VLAN Name
○ VID List (e.g.: 1, 4-6)
○ Port List (e.g.: 1:1, 1:3-1:5)
Find
View All

Total Entries: 1

Port	
1:20	Packet Statistics

Figure 4-66 MLD Snooping Counter window

The fields that can be configured are described below:

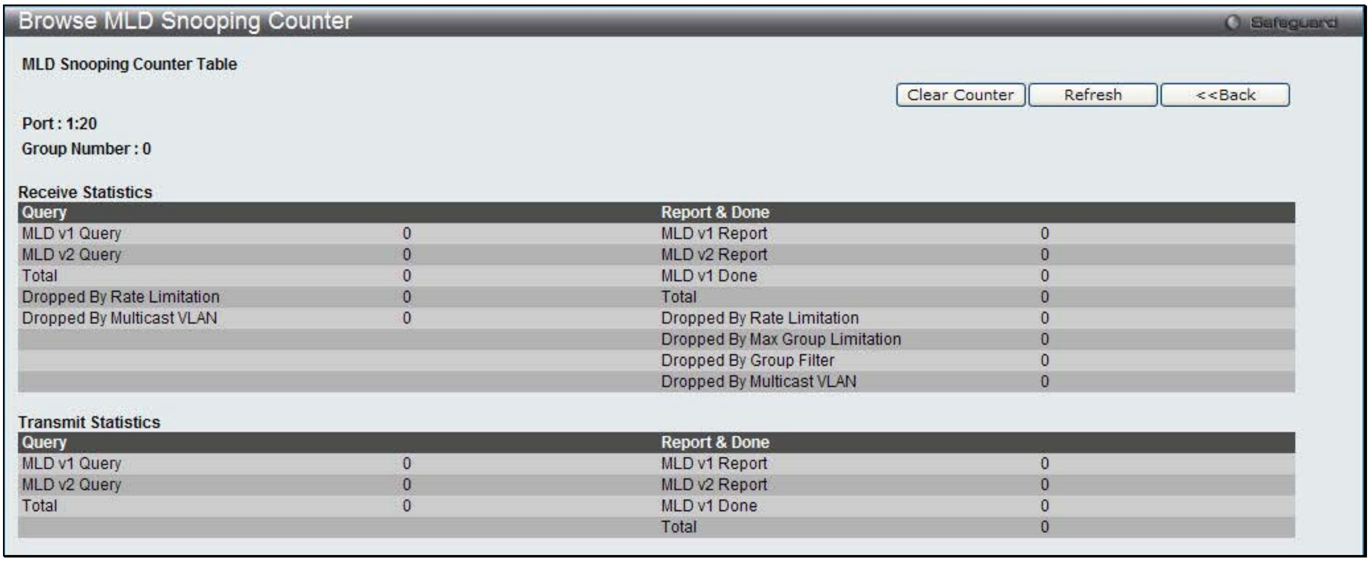
Parameter	Description
VLAN Name	Specify a VLAN name to be displayed.
VID List	Specify a list of VLANs to be displayed.
Port List	Specify a list of ports to be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the Packet Statistics link to view the MLD Snooping Counter Settings for the specific entry.

After clicking the Packet Statistics link, the following page will appear:



MLD Snooping Counter Table

Port : 1:20

Group Number : 0

Receive Statistics

Query		Report & Done	
MLD v1 Query	0	MLD v1 Report	0
MLD v2 Query	0	MLD v2 Report	0
Total	0	MLD v1 Done	0
Dropped By Rate Limitation	0	Total	0
Dropped By Multicast VLAN	0	Dropped By Rate Limitation	0
		Dropped By Max Group Limitation	0
		Dropped By Group Filter	0
		Dropped By Multicast VLAN	0

Transmit Statistics

Query		Report & Done	
MLD v1 Query	0	MLD v1 Report	0
MLD v2 Query	0	MLD v2 Report	0
Total	0	MLD v1 Done	0
		Total	0

Figure 4-67 Browse MLD Snooping Counter window

Click the **Clear Counter** button to clear all the information displayed in the fields.

Click the **Refresh** button to refresh the display table so that new information will appear.

Click the **<<Back** button to return to the previous page.

Multicast VLAN

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

Restrictions and Provisos:

The Multicast VLAN feature of this Switch does have some restrictions and limitations, such as:

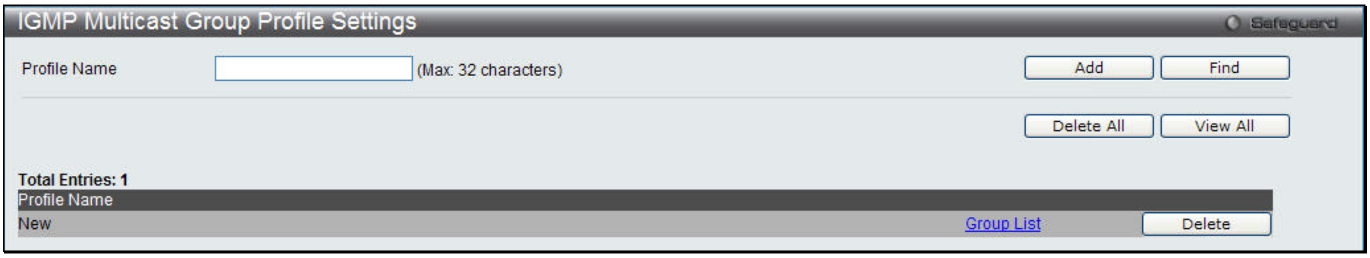
1. Multicast VLANs can be implemented on edge and non-edge switches.
2. Member ports and source ports can be used in multiple ISM VLANs. But member ports and source ports cannot be the same port in a specific ISM VLAN.
3. The Multicast VLAN is exclusive with normal 802.1q VLANs, which means that VLAN IDs (VIDs) and VLAN Names of 802.1q VLANs and ISM VLANs cannot be the same. Once a VID or VLAN Name is chosen for any VLAN, it cannot be used for any other VLAN.
4. The normal display of configured VLANs will not display configured Multicast VLANs.
5. Once an ISM VLAN is enabled, the corresponding IGMP snooping state of this VLAN will also be enabled. Users cannot disable the IGMP feature for an enabled ISM VLAN.
6. One IP multicast address cannot be added to multiple ISM VLANs, yet multiple Ranges can be added to one ISM VLAN.

IGMP Multicast Group Profile Settings

Users can add a profile to which multicast address reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the

Switch. The user may set an IP Multicast address or range of IP Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > IGMP Multicast Group Profile Settings**, as show below:


IGMP Multicast Group Profile Settings
Safeguard
Profile Name
(Max: 32 characters)
Add
Find
Delete All
View All
Group List
Delete

Total Entries: 1

Profile Name		
New	Group List	Delete

Figure 4-68 IGMP Multicast Group Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

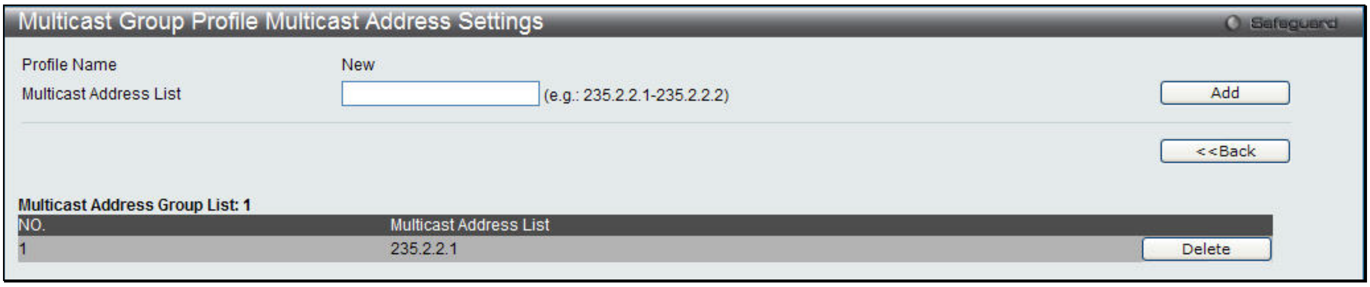
Click the **Delete All** button to remove all the entries listed.

Click the **View All** button to display all the existing entries.

Click the **Delete** button to remove the corresponding entry.

Click the Group List link to configure the Multicast Group Profile Address Settings for the specific entry.

After clicking the Group List link, the following page will appear:


Multicast Group Profile Multicast Address Settings
Safeguard
Multicast Address List
(e.g.: 235.2.2.1-235.2.2.2)
Add
<<Back
Delete

Profile Name New

Multicast Address Group List: 1

NO.	Multicast Address List	
1	235.2.2.1	Delete

Figure 4-69 Multicast Group Profile Multicast Address Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Enter the multicast address list value.

Click the **Add** button to add a new entry based on the information entered.

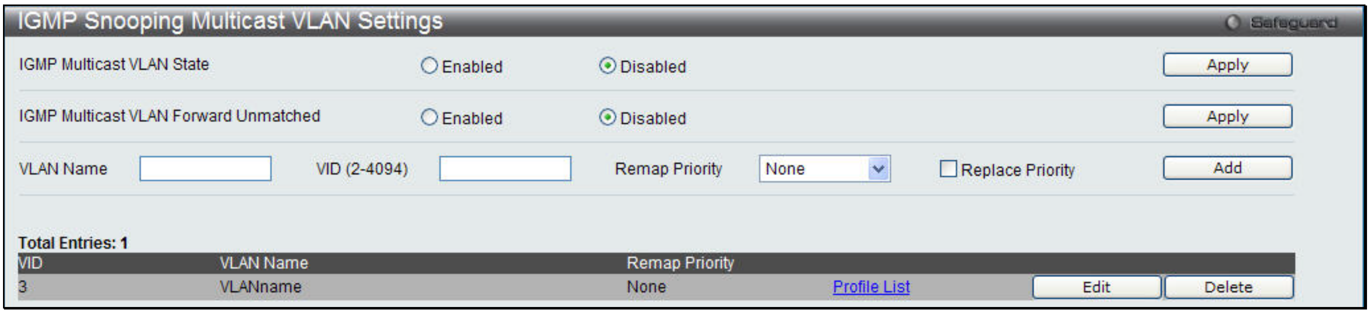
Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Delete** button to remove the corresponding entry.

IGMP Snooping Multicast VLAN Settings

On this page the user can configure the IGMP snooping multicast VLAN parameters.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > IGMP Snooping Multicast Group VLAN Settings**, as show below:


IGMP Snooping Multicast VLAN Settings
Safeguard
Apply
Apply
Add
Profile List
Edit
Delete

IGMP Multicast VLAN State ○ Enabled ● Disabled

IGMP Multicast VLAN Forward Unmatched ○ Enabled ● Disabled

VLAN Name ______ VID (2-4094) ______ Remap Priority None ☐ Replace Priority

Total Entries: 1

VID	VLAN Name	Remap Priority			
3	VLANname	None	Profile List	Edit	Delete

Figure 4-70 IGMP Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
IGMP Multicast VLAN State	Click the radio buttons to enable or disable the IGMP Multicast VLAN state.
IGMP Multicast VLAN Forward Unmatched	Click the radio buttons to enable or disable the IGMP Multicast VLAN Forwarding Unmatched state.
VLAN Name	Enter the VLAN Name used.
VID (2-4094)	Enter the VID used.
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If this is specified, the packet's original priority is used. The default setting is None.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Click the **Apply** button to accept the changes made for each individual section.

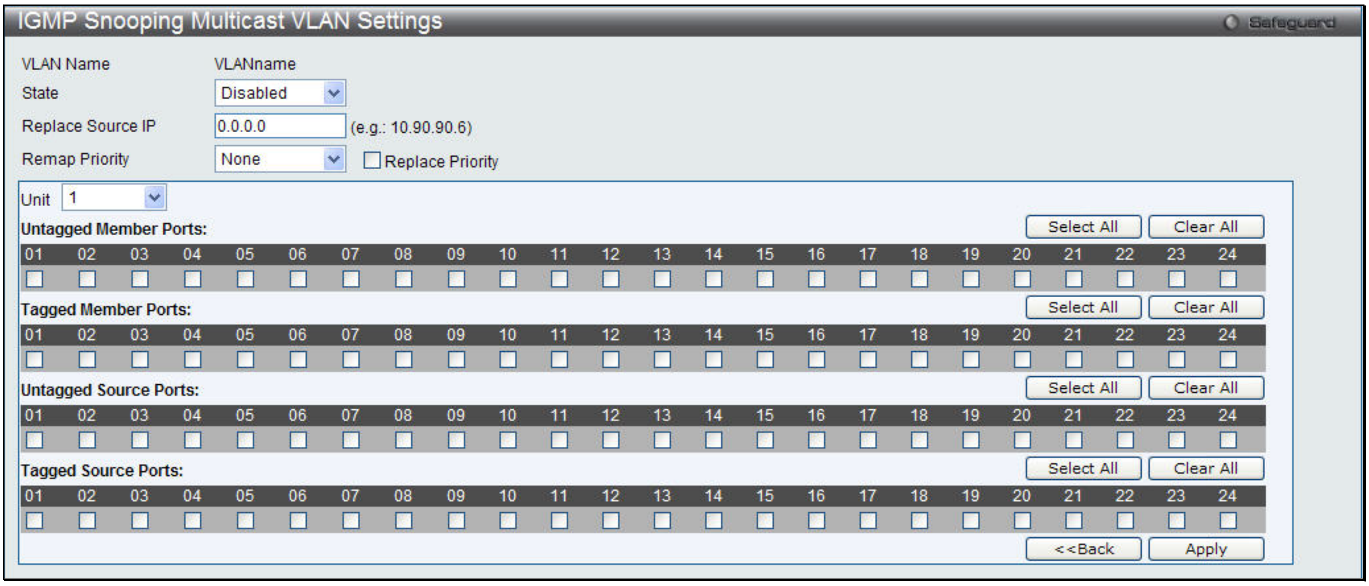
Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to configure the IGMP Snooping Multicast VLAN Settings for the specific entry.

Click the **Delete** button to remove the specific entry.

Click the Profile List link to configure the IGMP Snooping Multicast VLAN Settings for the specific entry.

After clicking the **Edit** button, the following page will appear:


IGMP Snooping Multicast VLAN Settings
Safeguard
Untagged Member Ports:
Tagged Member Ports:
Untagged Source Ports:
Tagged Source Ports:
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Select All
Clear All
<<Back
Apply

VLAN Name VLANname

State Disabled

Replace Source IP 0.0.0.0 (e.g.: 10.90.90.6)

Remap Priority None ☐ Replace Priority

Unit 1

Figure 4-71 IGMP Snooping Multicast VLAN Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
State	Use the drop-down menu to enable or disable the state.
Replace Source IP	With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced.
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If **None** is specified, the packet's original priority is used. The default setting is None.
Replace Priority	Specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.
Unit	Select the unit you want to configure.
Untagged Member Ports	Specify the untagged member port of the multicast VLAN.
Tagged Member Ports	Specify the tagged member port of the multicast VLAN.
Untagged Source Ports	Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.
Tagged Source Ports	Specify the source port or range of source ports as tagged members of the multicast VLAN.

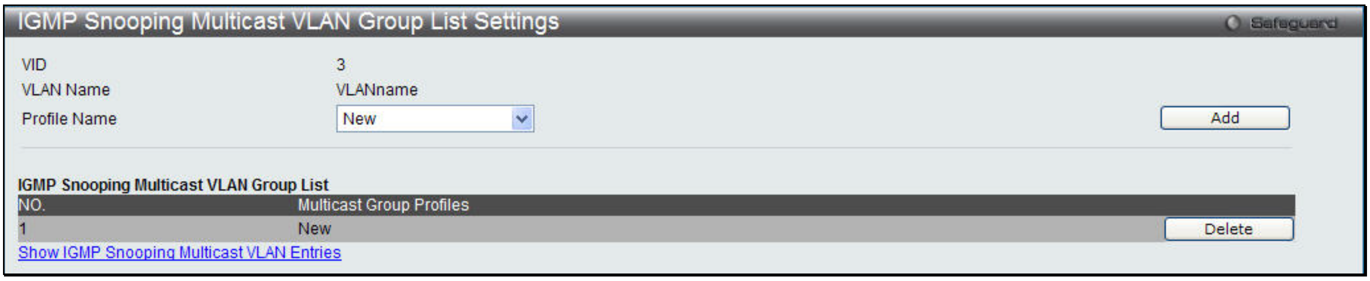
Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the Profile List link, the following page will appear:


IGMP Snooping Multicast VLAN Group List Settings
Safeguard
Add
Delete
Show IGMP Snooping Multicast VLAN Entries

VID 3

VLAN Name VLANname

Profile Name New

IGMP Snooping Multicast VLAN Group List

NO.	Multicast Group Profiles
1	New

Figure 4-72 IGMP Snooping Multicast VLAN Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Use the drop-down menu to select the IGMP Snooping Multicast VLAN Group Profile name.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

Click the Show IGMP Snooping Multicast VLAN Entries link to view the IGMP Snooping Multicast VLAN Settings.

MLD Multicast Group Profile Settings

Users can add, delete, or configure the MLD multicast group profile on this page.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > MLD Multicast Group Profile Settings**, as show below:

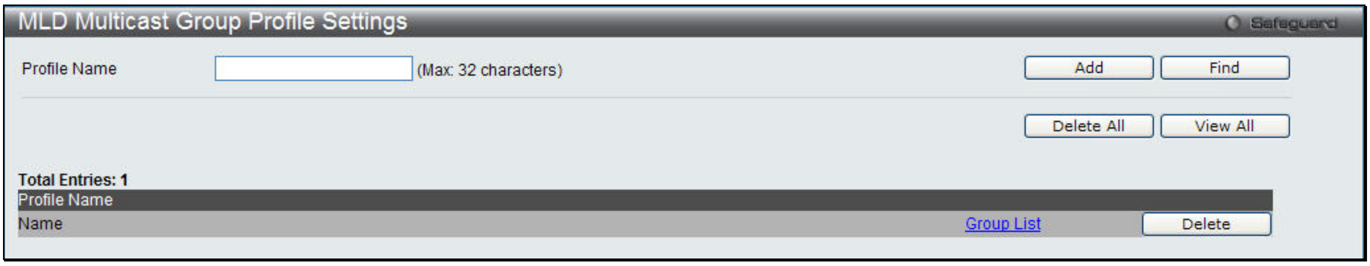

MLD Multicast Group Profile Settings
Safeguard
Profile Name
(Max: 32 characters)
Add
Find
Delete All
View All
Total Entries: 1
Profile Name
Name
Group List
Delete

Figure 4-73 MLD Multicast Group Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Enter the MLD Multicast Group Profile name.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Click the **View All** button to display all the existing entries.

Click the Group List link to configure the Multicast Group Profile Multicast Address Settings for the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:

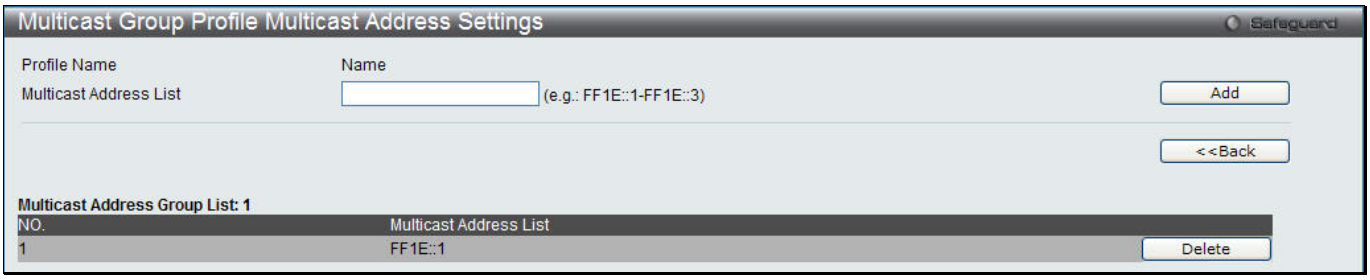

Multicast Group Profile Multicast Address Settings
Safeguard
Profile Name
Name
Multicast Address List
(e.g.: FF1E::1-FF1E::3)
Add
<<Back
Multicast Address Group List: 1
NO.
Multicast Address List
1
FF1E::1
Delete

Figure 4-74 Multicast Group Profile Multicast Address Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Enter the multicast address list.

Click the **Add** button to add a new entry based on the information entered.

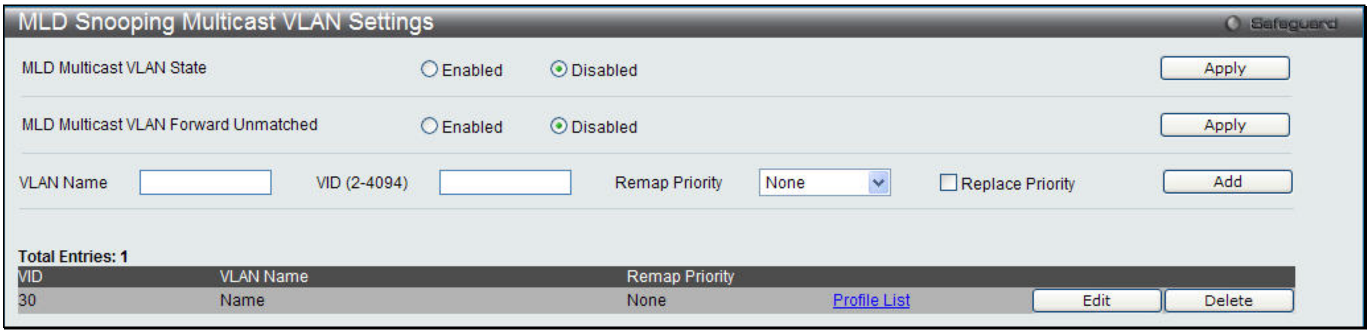
Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Delete** button to remove the specific entry.

MLD Snooping Multicast VLAN Settings

Users can add, delete, or configure the MLD snooping multicast VLAN on this page.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast VLAN > MLD Snooping Multicast Group VLAN Settings**, as show below:



MLD Multicast VLAN State ○ Enabled ● Disabled

MLD Multicast VLAN Forward Unmatched ○ Enabled ● Disabled

VLAN Name VID (2-4094) Remap Priority None ☐ Replace Priority

Total Entries: 1

VID	VLAN Name	Remap Priority			
30	Name	None	Profile List	Edit	Delete

Figure 4-75 MLD Snooping Multicast VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
MLD Multicast VLAN State	Click the radio buttons to enable or disable the MLD multicast VLAN state.
MLD Multicast VLAN Forward Unmatched	Click the radio buttons to can enable or disable the MLD multicast VLAN Forward Unmatched state.
VLAN Name	Enter the VLAN name used.
VID (2-4094)	Enter the VID value used.
Remap Priority	The user can select this option to enable the Remap Priority feature. Specify the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. If **None** is specified, the packet's original priority will be used. The default setting is None.
Replace Priority	Tick the check box to specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.

Click the **Apply** button to accept the changes made for each individual section.

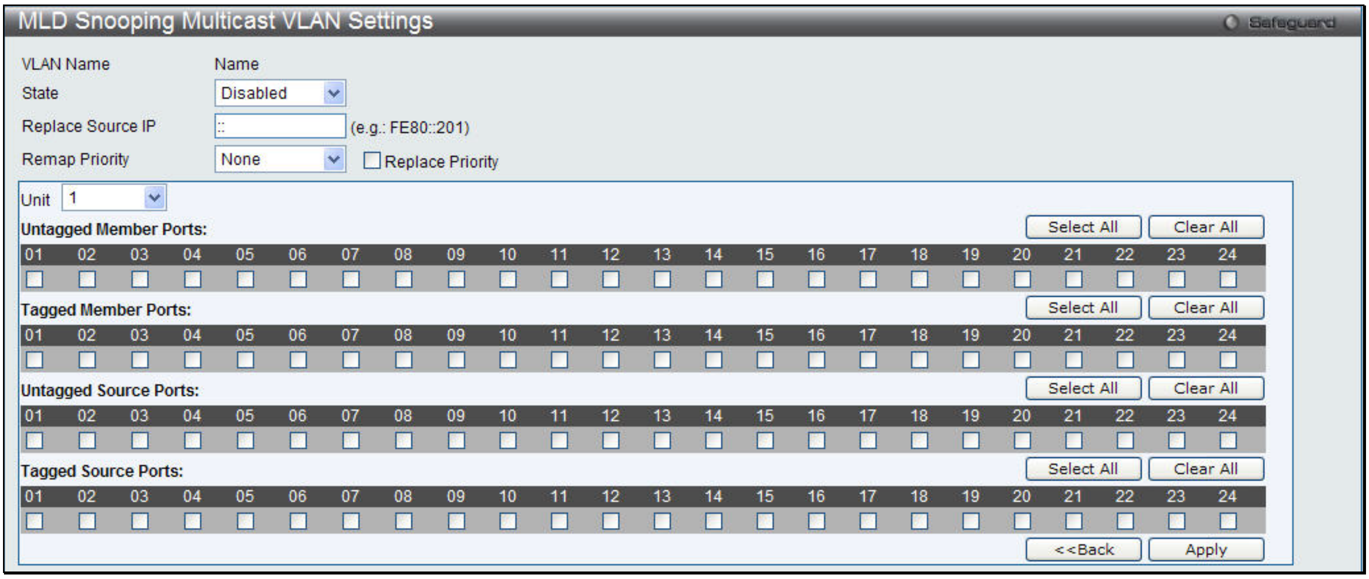
Click the **Add** button to add a new entry based on the information entered.

Click the **Edit** button to configure the MLD Snooping Multicast VLAN Settings for the specific entry.

Click the **Delete** button to remove the specific entry.

Click the Profile List link to configure the MLD Snooping Multicast VLAN Settings for the specific entry.

After clicking the **Edit** button, the following page will appear:



VLAN Name Name

State Disabled

Replace Source IP :: (e.g.: FE80::201)

Remap Priority None ☐ Replace Priority

Unit 1

Untagged Member Ports:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Tagged Member Ports:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Untagged Source Ports:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Tagged Source Ports:

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Figure 4-76 MLD Snooping Multicast VLAN Settings – Edit window

The fields that can be configured are described below:

Parameter	Description
State	Use the drop-down menu to enable or disable the state.
Replace Source IP	With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address. If none is specified, the source IP address will not be replaced.
Remap Priority	*0-7* – The remap priority value (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. *None* – If this is specified, the packet's original priority is used. The default setting is *None*.
Replace Priority	Tick the check box to specify that the packet's priority will be changed by the switch, based on the remap priority. This flag will only take effect when the remap priority is set.
Unit	Select the unit you want to configure.
Untagged Member Ports	Specify the untagged member port of the multicast VLAN.
Tagged Member Ports	Specify the tagged member port of the multicast VLAN.
Untagged Source Ports	Specify the source port or range of source ports as untagged members of the multicast VLAN. The PVID of the untagged source port is automatically changed to the multicast VLAN. Source ports must be either tagged or untagged for any single multicast VLAN, i.e. both types cannot be members of the same multicast VLAN.
Tagged Source Ports	Specify the source port or range of source ports as tagged members of the multicast VLAN.

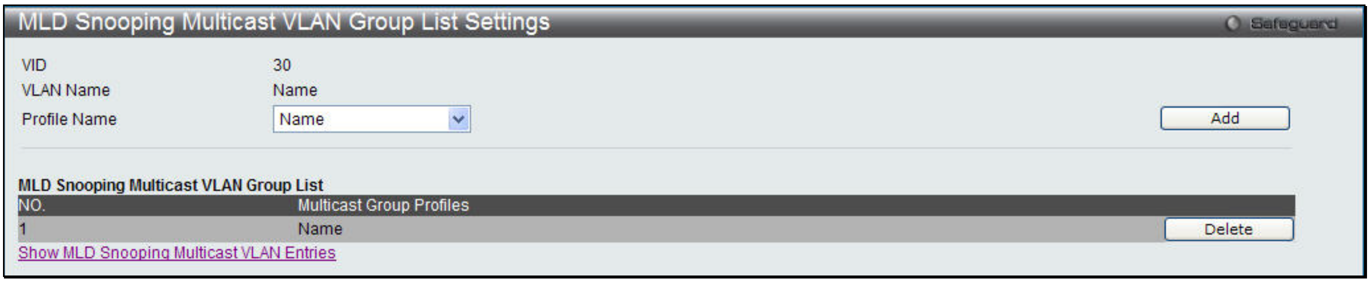
Click the **Select All** button to select all the ports for configuration.

Click the **Clear All** button to unselect all the ports for configuration.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the Profile List link, the following page will appear:



VID 30

VLAN Name Name

Profile Name Name

MLD Snooping Multicast VLAN Group List

NO.	Multicast Group Profiles
1	Name

Show MLD Snooping Multicast VLAN Entries

Figure 4-77 MLD Snooping Multicast VLAN Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Profile Name	Use the drop-down menu to select the IGMP Snooping Multicast VLAN Group Profile name.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

Click the Show MLD Snooping Multicast VLAN Entries link to view the MLD Snooping Multicast VLAN Settings.

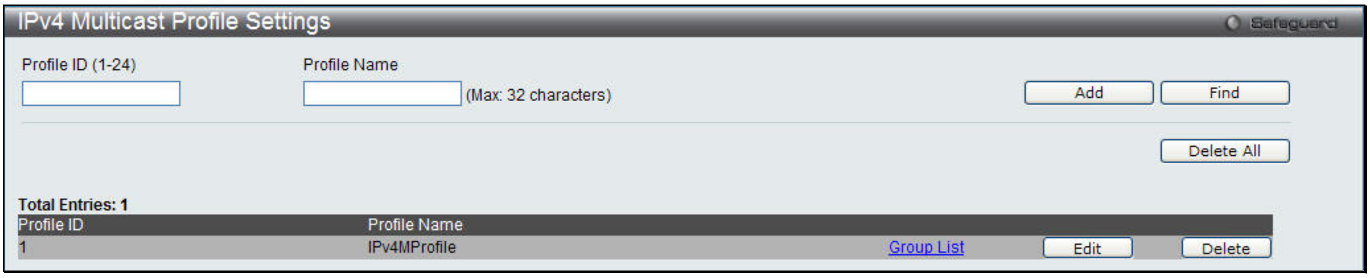
Multicast Filtering

IPv4 Multicast Filtering

IPv4 Multicast Profile Settings

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IPv4 Multicast address or range of IPv4 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings**, as show below:


IPv4 Multicast Profile Settings
Safeguard
Profile ID (1-24)
Profile Name
(Max: 32 characters)
Add
Find
Delete All

Total Entries: 1

Profile ID	Profile Name			
1	IPv4MProfile	Group List	Edit	Delete

Figure 4-78 IPv4 Multicast Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-24)	Enter a Profile ID between *1* and *24*.
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

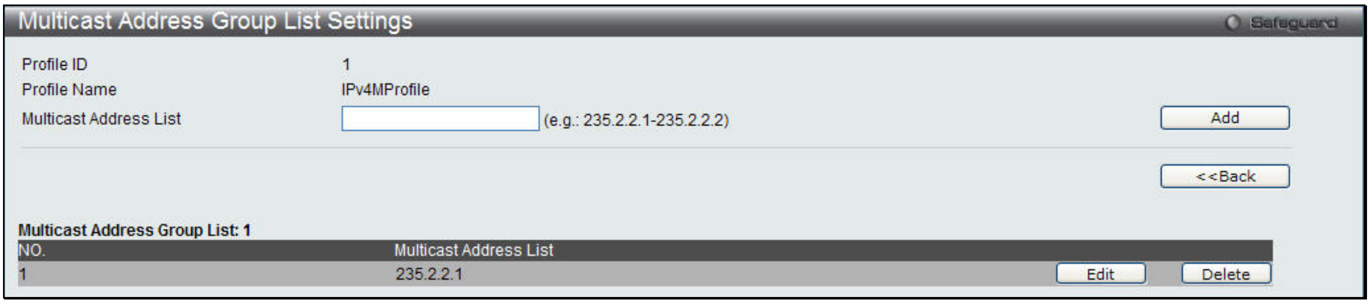
Click the **Delete All** button to remove all the entries listed.

Click the Group List link to configure the multicast address group list settings for the specific entry.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:


Multicast Address Group List Settings
Safeguard
Multicast Address List
(e.g.: 235.2.2.1-235.2.2.2)
Add
<<Back

Profile ID 1

Profile Name IPv4MProfile

Multicast Address Group List: 1

NO.	Multicast Address List		
1	235.2.2.1	Edit	Delete

Figure 4-79 Multicast Address Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Multicast Address List	Enter the multicast address list.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

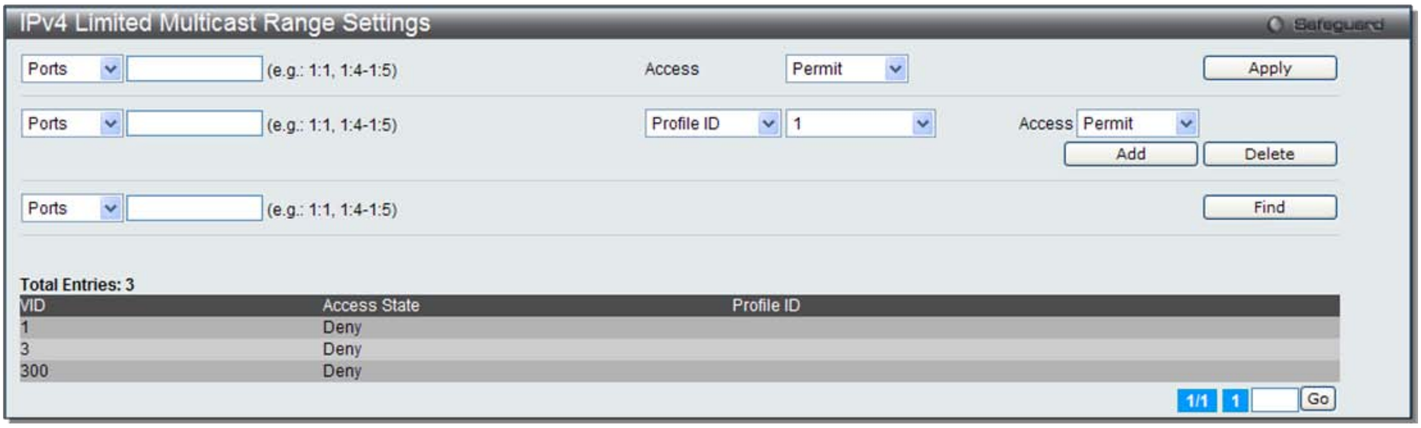
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

IPv4 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv4 Multicast Range. The user can configure the range of multicast ports that will be accepted by the source ports to be forwarded to the receiver ports.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings**, as show below:



Ports (e.g.: 1:1, 1:4-1:5) Access: Permit

Ports (e.g.: 1:1, 1:4-1:5) Profile ID: 1 Access: Permit

Ports (e.g.: 1:1, 1:4-1:5)

Total Entries: 3

VID	Access State	Profile ID
1	Deny	
3	Deny	
300	Deny	

Figure 4-80 IPv4 Limited Multicast Range Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration.
Access	Assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name	Use the drop-down menu to select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry.

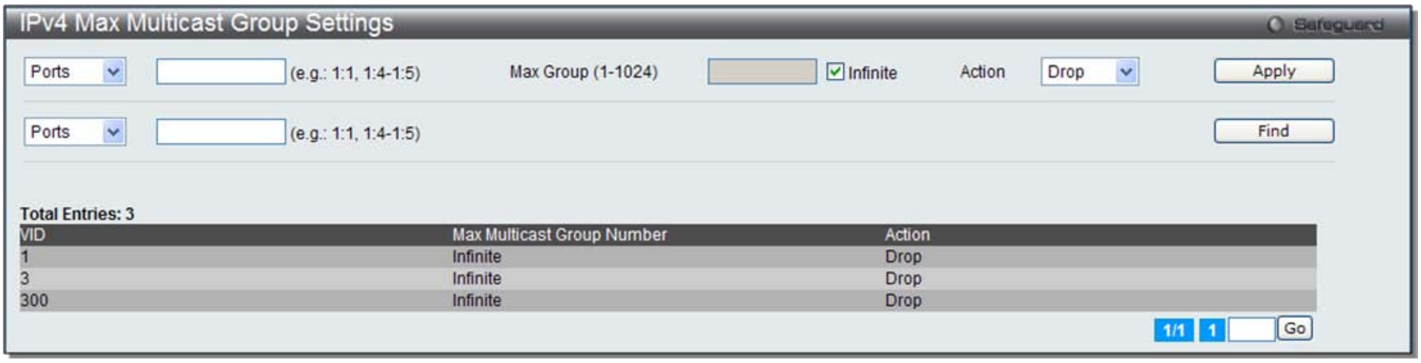
Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv4 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.

To view the following window, click **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Max Multicast Group Settings**, as show below:


IPv4 Max Multicast Group Settings
Safeguard
Ports
(e.g.: 1:1, 1:4-1:5)
Max Group (1-1024)
☑ Infinite
Action
Drop
Apply
Ports
(e.g.: 1:1, 1:4-1:5)
Find
1/1
1
Go

Total Entries: 3

VID	Max Multicast Group Number	Action
1	Infinite	Drop
3	Infinite	Drop
300	Infinite	Drop

Figure 4-81 IPv4 Max Multicast Group Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group (1-1024)	If the checkbox **Infinite** is not selected, the user can enter a **Max Group** value.
Infinite	Tick the check box to enable or disable the use of the Infinite value.
Action	Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

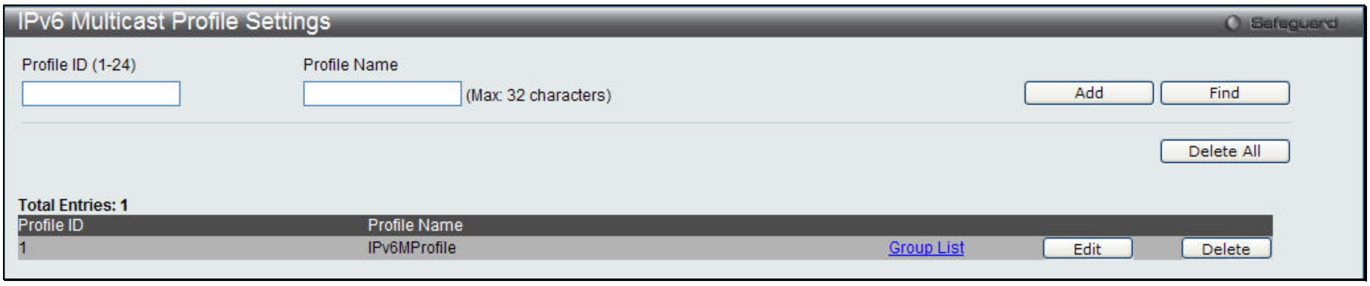
IPv6 Multicast Filtering

Users can add a profile to which multicast address(s) reports are to be received on specified ports on the Switch. This function will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IPv6 Multicast address or range of IPv6 Multicast addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

IPv6 Multicast Profile Settings

Users can add, delete, and configure the IPv6 multicast profile on this page.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Profile Settings**, as show below:


IPv6 Multicast Profile Settings
Safeguard
Profile ID (1-24)
Profile Name
(Max: 32 characters)
Add
Find
Delete All
Group List
Edit
Delete

Total Entries: 1

Profile ID	Profile Name
1	IPv6MProfile

Figure 4-82 IPv4 Multicast Profile Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-24)	Enter a Profile ID between *1* and *24*.
Profile Name	Enter a name for the IP Multicast Profile.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

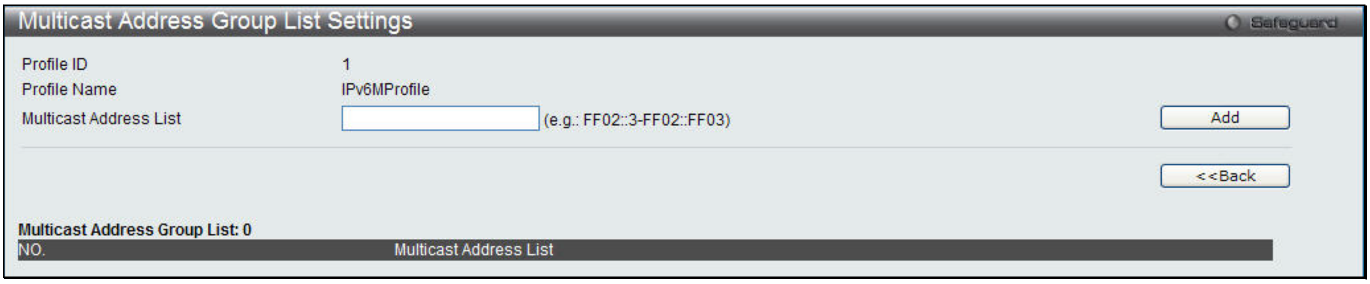
Click the **Delete All** button to remove all the entries listed.

Click the Group List link to configure the multicast address group list settings for the specific entry.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the Group List link, the following page will appear:


Multicast Address Group List Settings
Safeguard
(e.g.: FF02::3-FF02::FF03)
Add
<<Back

Profile ID: 1

Profile Name: IPv6MProfile

Multicast Address List:

Multicast Address Group List: 0

NO.	Multicast Address List

Figure 4-83 Multicast Address Group List Settings window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Display the profile ID.
Profile Name	Display the profile name.
Multicast Address List	Enter the multicast address list here.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

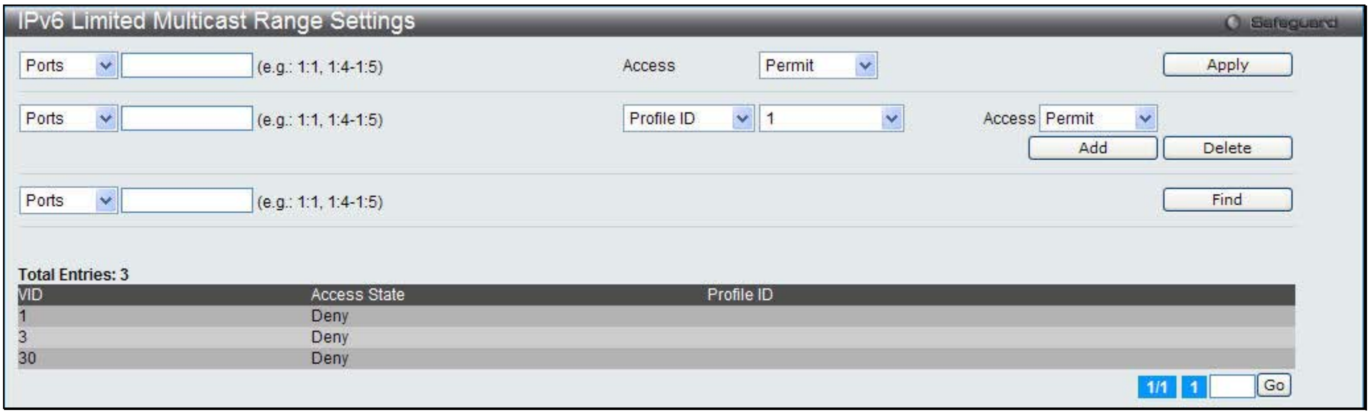
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

IPv6 Limited Multicast Range Settings

Users can configure the ports and VLANs on the Switch that will be involved in the Limited IPv6 Multicast Range.

To view the following window, click **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings**, as show below:


IPv6 Limited Multicast Range Settings
Safeguard
(e.g.: 1:1, 1:4-1:5)
(e.g.: 1:1, 1:4-1:5)
(e.g.: 1:1, 1:4-1:5)
Apply
Add
Delete
Find
1/1
1
Go

Ports — Access: Permit

Ports — Profile ID: 1 — Access: Permit

Ports

Total Entries: 3

VID	Access State	Profile ID
1	Deny	
3	Deny	
30	Deny	

Figure 4-84 IPv6 Limited Multicast Range Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration here.

Access	Assign access permissions to the ports selected. Options listed are **Permit** and **Deny**.
Profile ID / Profile Name	Use the drop-down menu to select the profile ID or profile name used and then assign **Permit** or **Deny** access to them.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

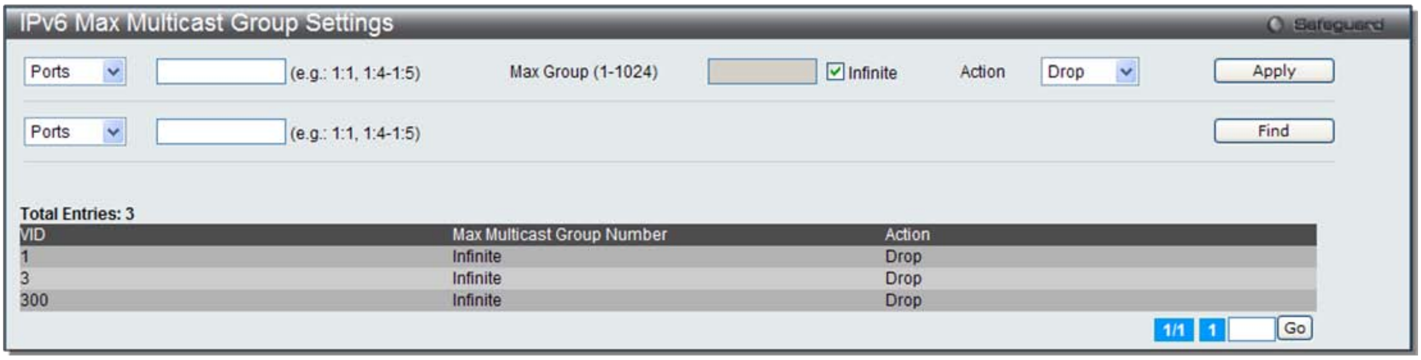
Click the **Delete** button to remove the specific entry.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Max Multicast Group Settings

Users can configure the ports and VLANs on the switch that will be a part of the maximum filter group, up to a maximum of 1024.



Total Entries: 3

VID	Max Multicast Group Number	Action
1	Infinite	Drop
3	Infinite	Drop
300	Infinite	Drop

Figure 4-85 IPv4 Max Multicast Group Settings window

The fields that can be configured are described below:

Parameter	Description
Ports / VID List	Select the appropriate port(s) or VLAN IDs used for the configuration here.
Max Group	If the checkbox **Infinite** is not selected, the user can enter a **Max Group** value.
Infinite	Tick the check box to enable or disable the use of the Infinite value.
Action	Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click the **Apply** button to accept the changes made.

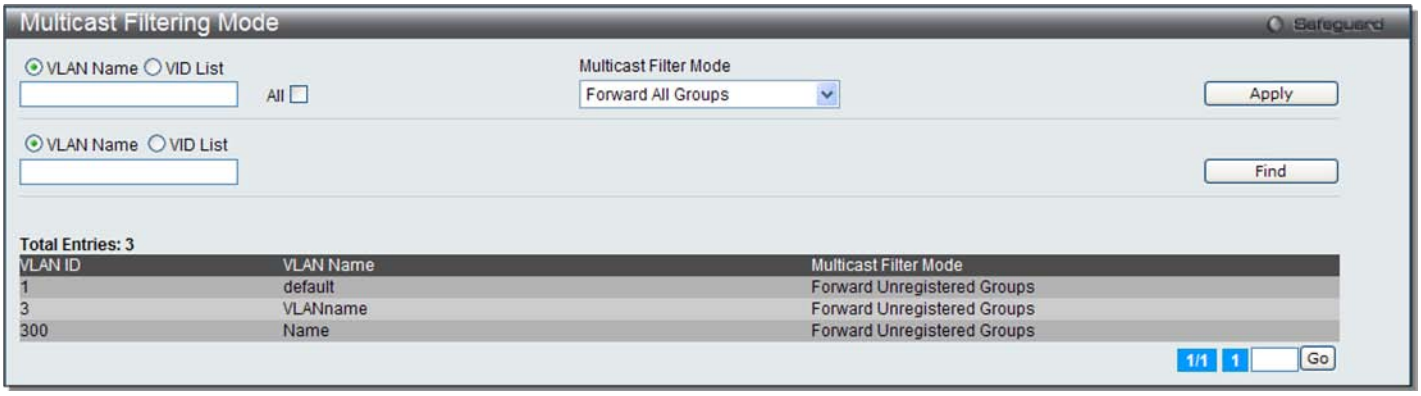
Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Multicast Filtering Mode

Users can configure the multicast filtering mode.

To view the following window, click **L2 Features > Multicast Filtering > Multicast Filtering Mode**, as show below:



● VLAN Name ○ VID List

All ☐

Multicast Filter Mode: Forward All Groups

● VLAN Name ○ VID List

Total Entries: 3

VLAN ID	VLAN Name	Multicast Filter Mode
1	default	Forward Unregistered Groups
3	VLANname	Forward Unregistered Groups
300	Name	Forward Unregistered Groups

Figure 4-86 Multicast Filtering Mode window

The fields that can be configured are described below:

Parameter	Description
VLAN Name / VID List	The VLAN to which the specified filtering action applies. Tick the **All** check box to apply this feature to all the VLANs.
Multicast Filtering Mode	This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN. *Forward All Groups* – This will instruct the Switch to forward all multicast packets to the specified VLAN. *Forward Unregistered Groups* – The multicast packets whose destination is an unregistered multicast group will be forwarded within the range of ports specified above. *Filter Unregistered Groups* – The multicast packets whose destination is a registered multicast group will be forwarded within the range of ports specified above.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ERPS Settings (EI Mode Only)

ERPS (Ethernet Ring Protection Switching) is the first industry standard (ITU-T G.8032) for Ethernet ring protection switching. It is achieved by integrating mature Ethernet operations, administration, and maintenance (OAM) * functions and a simple automatic protection switching (APS) protocol for Ethernet ring networks. ERPS provides sub-50ms protection for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring will be blocked to avoid Loop (RPL, Ring Protection Link). When the failure happens, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

G.8032 Terms and Concepts

RPL (Ring Protection Link) – Link designated by mechanism that is blocked during Idle state to prevent loop on Bridged ring

RPL Owner – Node connected to RPL that blocks traffic on RPL during Idle state and unblocks during Protected state

R-APS (Ring – Automatic Protection Switching) - Protocol messages defined in Y.1731 and G.8032 used to coordinate the protection actions over the ring through RAPS VLAN (R-APS Channel).

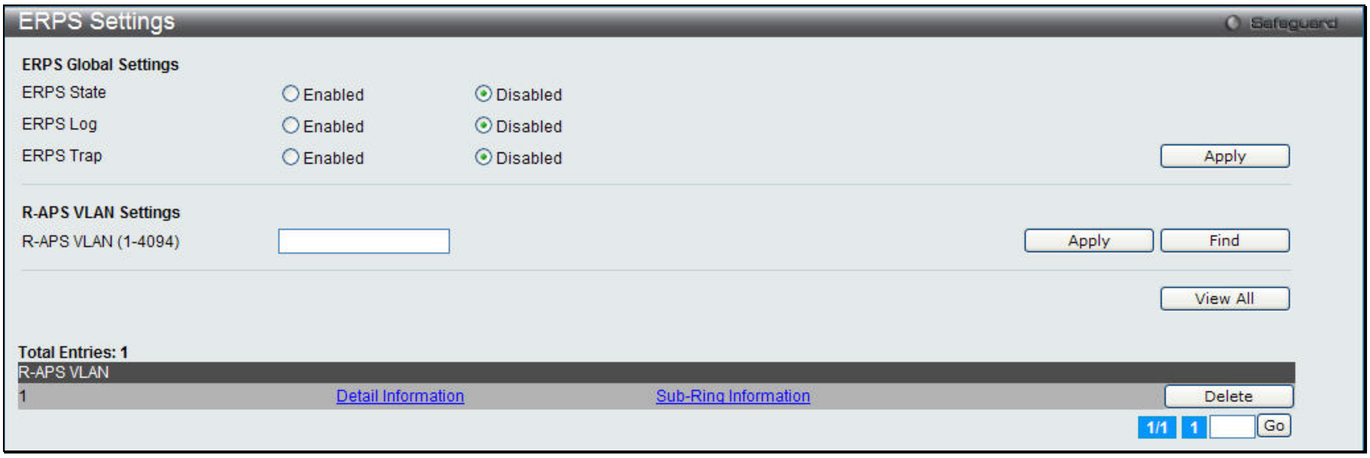
RAPS VLAN (R-APS Channel) – A separate ring-wide VLAN for transmission of R-APS messages

Protected VLAN – The service traffic VLANs for transmission of normal network traffic

This page is used to enable the ERPS function on the switch.

NOTE: STP and LBD should be disabled on the ring ports before enabling ERPS. The ERPS cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when ERPS is enabled.

To view the following window, click **L2 Features > ERPS Settings**, as show below:



ERPS Global Settings

ERPS State ○ Enabled ● Disabled

ERPS Log ○ Enabled ● Disabled

ERPS Trap ○ Enabled ● Disabled

R-APS VLAN Settings

R-APS VLAN (1-4094)

Total Entries: 1

R-APS VLAN			
1	Detail Information	Sub-Ring Information	Delete

Figure 4-87 ERPS Settings Window

The fields that can be configured are described below:

Parameter	Description
ERPS State	Click to enable or disable the ERPS State.
ERPS Log	Click to enable or disable the ERPS Log.
ERPS Trap	Click to enable or disable the ERPS Trap.
R-APS VLAN (1-4094)	Specifies the VLAN which will be the R-APS VLAN.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Find** button to find a specific entry based on the information entered.

Click the **View All** button to view all the entries configured.

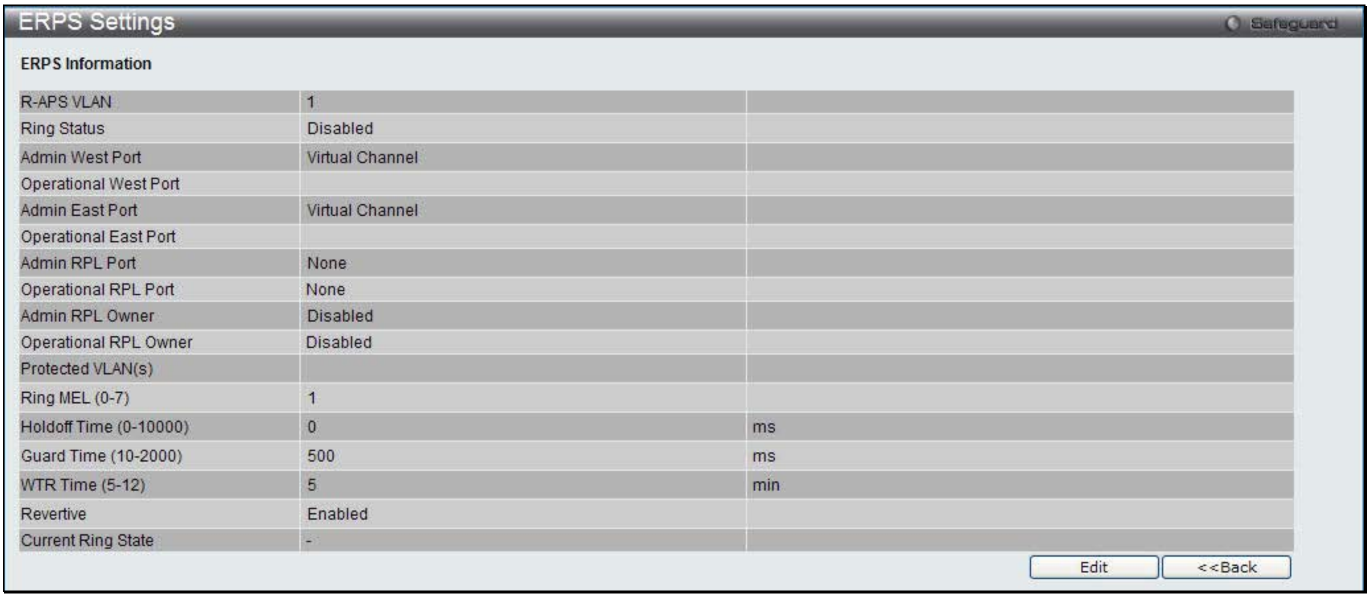
Click the **Delete** button to remove the specific entry.

Click the Detail Information link to view detailed information of the R-APS entry.

Click the Sub-Ring Information link to view the Sub-Ring information of the R-APS entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the Detail Information link, the following window will appear:



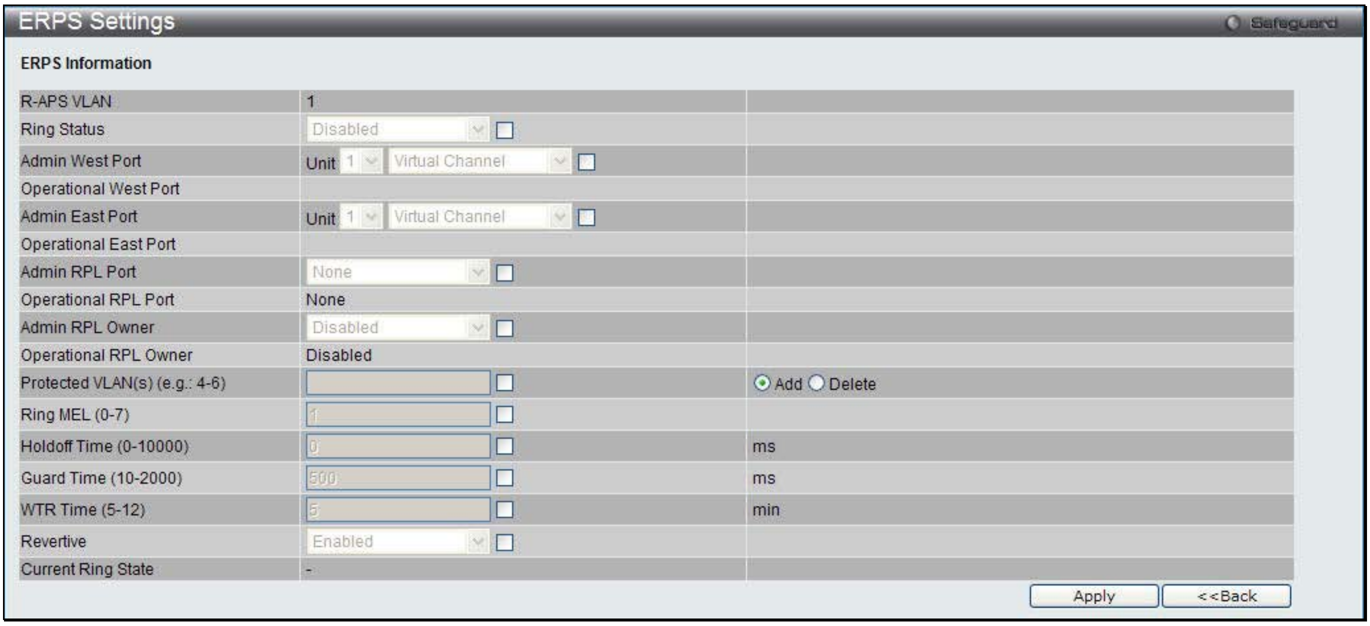
ERPS Information

R-APS VLAN	1	
Ring Status	Disabled	
Admin West Port	Virtual Channel	
Operational West Port		
Admin East Port	Virtual Channel	
Operational East Port		
Admin RPL Port	None	
Operational RPL Port	None	
Admin RPL Owner	Disabled	
Operational RPL Owner	Disabled	
Protected VLAN(s)		
Ring MEL (0-7)	1	
Holdoff Time (0-10000)	0	ms
Guard Time (10-2000)	500	ms
WTR Time (5-12)	5	min
Revertive	Enabled	
Current Ring State	-	

Figure 4-88 ERPS Settings - Detail Information window

Click on the **Edit** button to re-configure the specific entry.
Click on the **<<Back** button to return to the ERPS settings page.

After click the **Edit** button, the following window will appear:



ERPS Information

R-APS VLAN	1	
Ring Status	Disabled ☐	
Admin West Port	Unit 1 Virtual Channel ☐	
Operational West Port		
Admin East Port	Unit 1 Virtual Channel ☐	
Operational East Port		
Admin RPL Port	None ☐	
Operational RPL Port	None	
Admin RPL Owner	Disabled ☐	
Operational RPL Owner	Disabled	
Protected VLAN(s) (e.g.: 4-6)	☐	● Add ○ Delete
Ring MEL (0-7)	1 ☐	
Holdoff Time (0-10000)	0 ☐	ms
Guard Time (10-2000)	500 ☐	ms
WTR Time (5-12)	5 ☐	min
Revertive	Enabled ☐	
Current Ring State	-	

Figure 4-89 ERPS Settings - Edit Detail Information window

The fields that can be configured or displayed are described below:

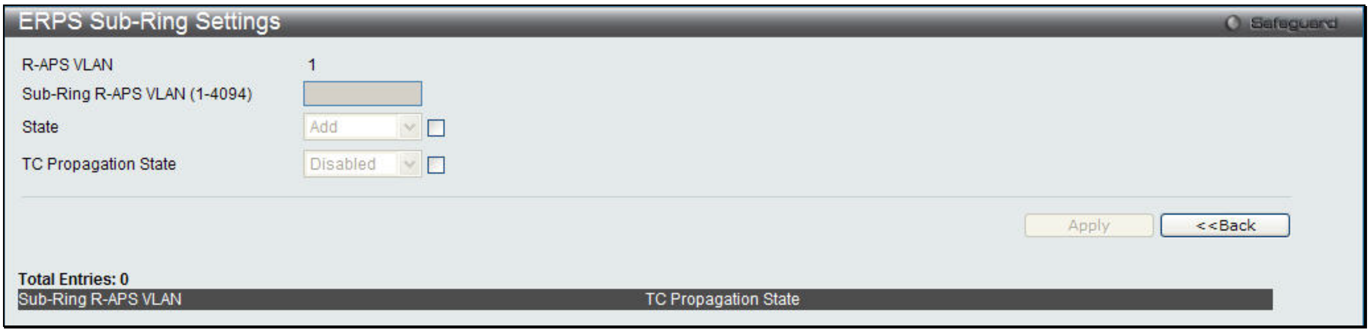
Parameter	Description
R-APS VLAN	Here the R-APS VLAN ID will be displayed.
Ring Status	Specifies to enable or disable the specified ring.
Admin West Port	Specifies the port as the west ring port and also specifies the virtual port channel used.
Operational West Port	Here the operational west port value will be displayed.
Admin East Port	Specifies the port as the east ring port and also specifies the virtual port channel used.

Operational East Port	Here the operational east port value will be displayed.
Admin RPL Port	Specifies the RPL port used. Options to choose from are **West Port**, **East Port**, and **None**.
Operational RPL Port	Here the operational RPL port value will be displayed.
Admin RPL Owner	Specifies to enable or disable the RPL owner node.
Operational RPL Owner	Here the operational RPL owner value will be displayed.
Protected VLAN(s)	Specifies to add or delete the protected VLAN group.
Ring MEL (0-7)	Specifies the ring MEL of the R-APS function. The default ring MEL is 1.
Holdoff Time (0-10000)	Specifies the hold-off time of the R-APS function. The default hold-off time is 0 milliseconds.
Guard Time (10-20000)	Specifies the guard time of the R-APS function. The default guard time is 500 milliseconds.
WTR Time (5-12)	Specifies the WTR time of the R-APS function.
Revertive	Specifies the state of the R-APS revertive option.
Current Ring State	Here the current Ring state will be displayed.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to return to the previous window.

After clicking the Sub-Ring Information link, the following window will appear:



R-APS VLAN 1

Sub-Ring R-APS VLAN (1-4094)

State Add ☐

TC Propagation State Disabled ☐

Total Entries: 0

Sub-Ring R-APS VLAN	TC Propagation State

Figure 4-90 ERPS Sub-Ring Settings window

The fields that can be configured are described below:

Parameter	Description
R-APS VLAN	Here the R-APS VLAN ID will be displayed.
Sub-Ring R-APS VLAN	Enter the Sub-Ring R-APS VLAN ID used here.
State	Specifies the ERPS Sub-Ring state here. Options to choose from are **Add** and **Delete**.
TC Propagation State	Specifies the TC Propagation state here. Options to choose from are **Enabled** and **Disabled**.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to return to the previous window.

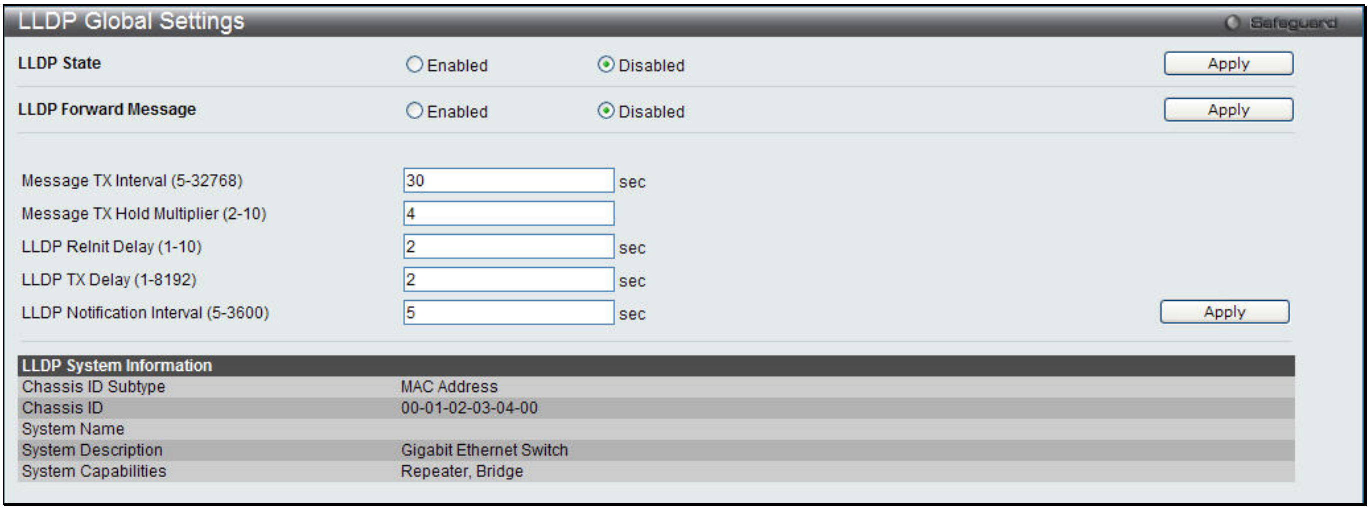
LLDP

LLDP

LLDP Global Settings

On this page the user can configure the LLDP global parameters.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Global Settings**, as show below:



LLDP State ○ Enabled ● Disabled

LLDP Forward Message ○ Enabled ● Disabled

Message TX Interval (5-32768): 30 sec

Message TX Hold Multiplier (2-10): 4

LLDP ReInit Delay (1-10): 2 sec

LLDP TX Delay (1-8192): 2 sec

LLDP Notification Interval (5-3600): 5 sec

LLDP System Information	
Chassis ID Subtype	MAC Address
Chassis ID	00-01-02-03-04-00
System Name	
System Description	Gigabit Ethernet Switch
System Capabilities	Repeater, Bridge

Figure 4-91 LLDP Global Settings window

The fields that can be configured are described below:

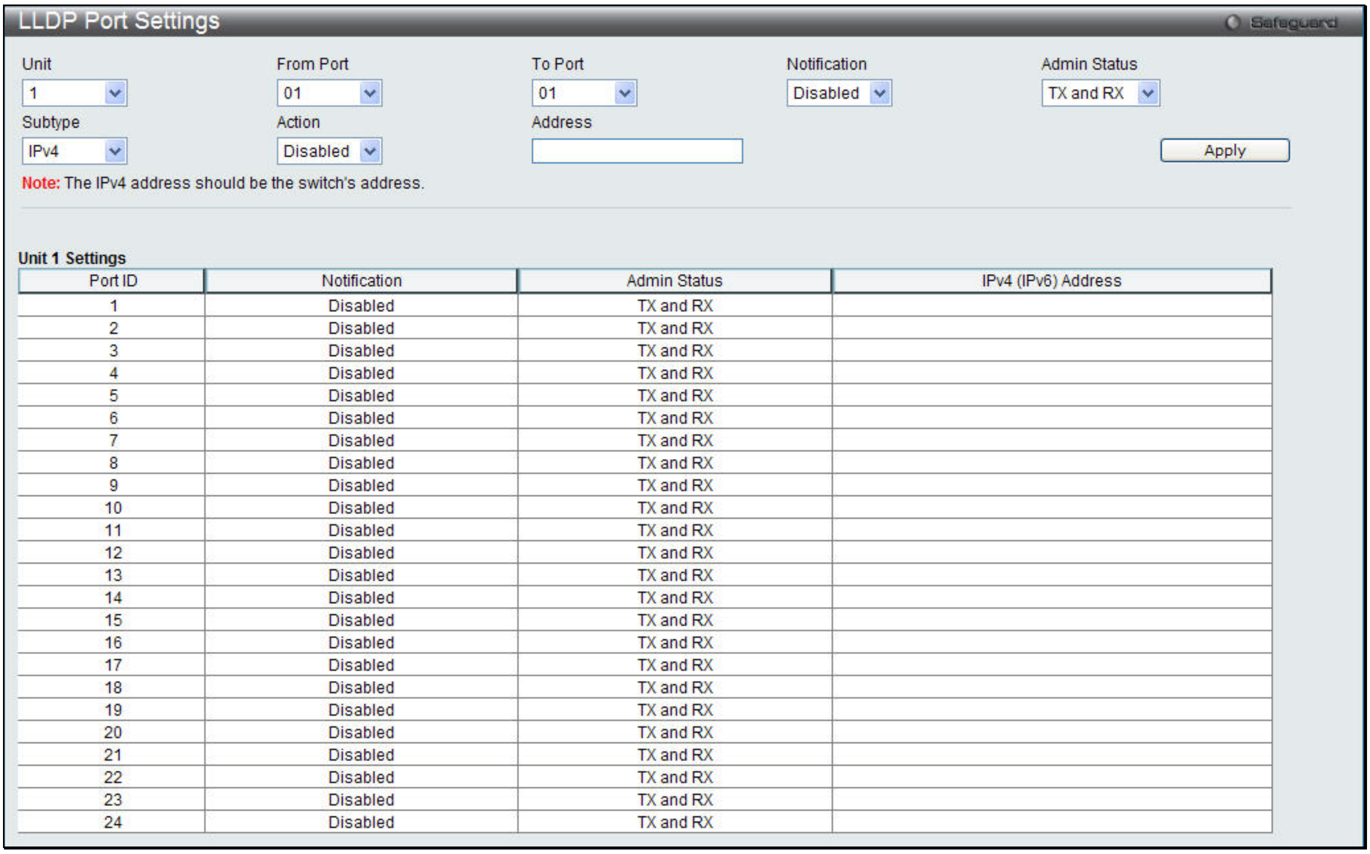
Parameter	Description
LLDP State	Click the radio buttons to enable or disable the LLDP feature.
LLDP Forward Message	When LLDP is disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message TX Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
LLDP ReInit Delay (1-10)	The LLDP re-initialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP re-init delay, enter a value in seconds (1 to 10).
LLDP TX Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
LLDP Notification interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

Click the **Apply** button to accept the changes made for each individual section.

LLDP Port Settings

On this page the user can configure the LLDP port parameters.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
Notification: Disabled
Admin Status: TX and RX
Subtype: IPv4
Action: Disabled
Address:

Note: The IPv4 address should be the switch's address.

Unit 1 Settings

Port ID	Notification	Admin Status	IPv4 (IPv6) Address
1	Disabled	TX and RX	
2	Disabled	TX and RX	
3	Disabled	TX and RX	
4	Disabled	TX and RX	
5	Disabled	TX and RX	
6	Disabled	TX and RX	
7	Disabled	TX and RX	
8	Disabled	TX and RX	
9	Disabled	TX and RX	
10	Disabled	TX and RX	
11	Disabled	TX and RX	
12	Disabled	TX and RX	
13	Disabled	TX and RX	
14	Disabled	TX and RX	
15	Disabled	TX and RX	
16	Disabled	TX and RX	
17	Disabled	TX and RX	
18	Disabled	TX and RX	
19	Disabled	TX and RX	
20	Disabled	TX and RX	
21	Disabled	TX and RX	
22	Disabled	TX and RX	
23	Disabled	TX and RX	
24	Disabled	TX and RX	

Figure 4-92 LLDP Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the ports used for this configuration.
Notification	Use the drop-down menu to enable or disable the status of the LLDP notification. This function controls the SNMP trap however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains **TX**, **RX**, **TX And RX** or **Disabled**. *TX* - the local LLDP agent can only transmit LLDP frames. *RX* - the local LLDP agent can only receive LLDP frames. *TX And RX* - the local LLDP agent can both transmit and receive LLDP frames. *Disabled* - the local LLDP agent can neither transmit nor receive LLDP frames. The default value is TX And RX.
Subtype	Use the drop-down menu to select the type of the IP address information will be sent.
Action	Use the drop-down menu to enable or disable the action field.
Address	Enter the IP address that will be sent.

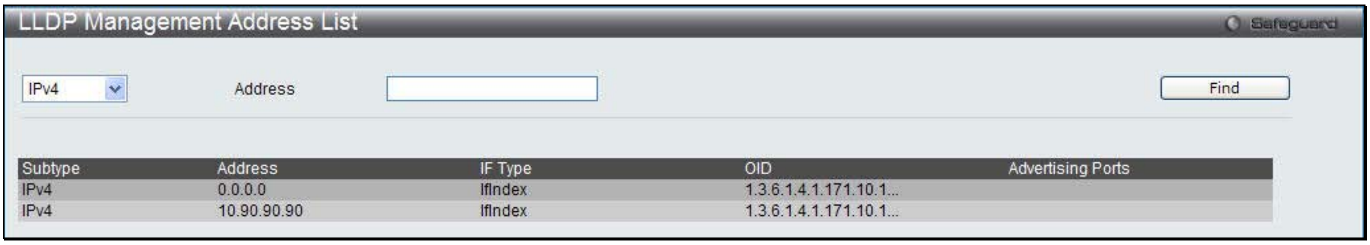
Click the **Apply** button to accept the changes made.

NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

LLDP Management Address List

On this page the user can view the LLDP management address list.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP management Address List**, as show below:



Subtype	Address	IF Type	OID	Advertising Ports
IPv4	0.0.0.0	IfIndex	1.3.6.1.4.1.171.10.1...	
IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.171.10.1...	

Figure 4-93 LLDP Management Address List window

The fields that can be configured are described below:

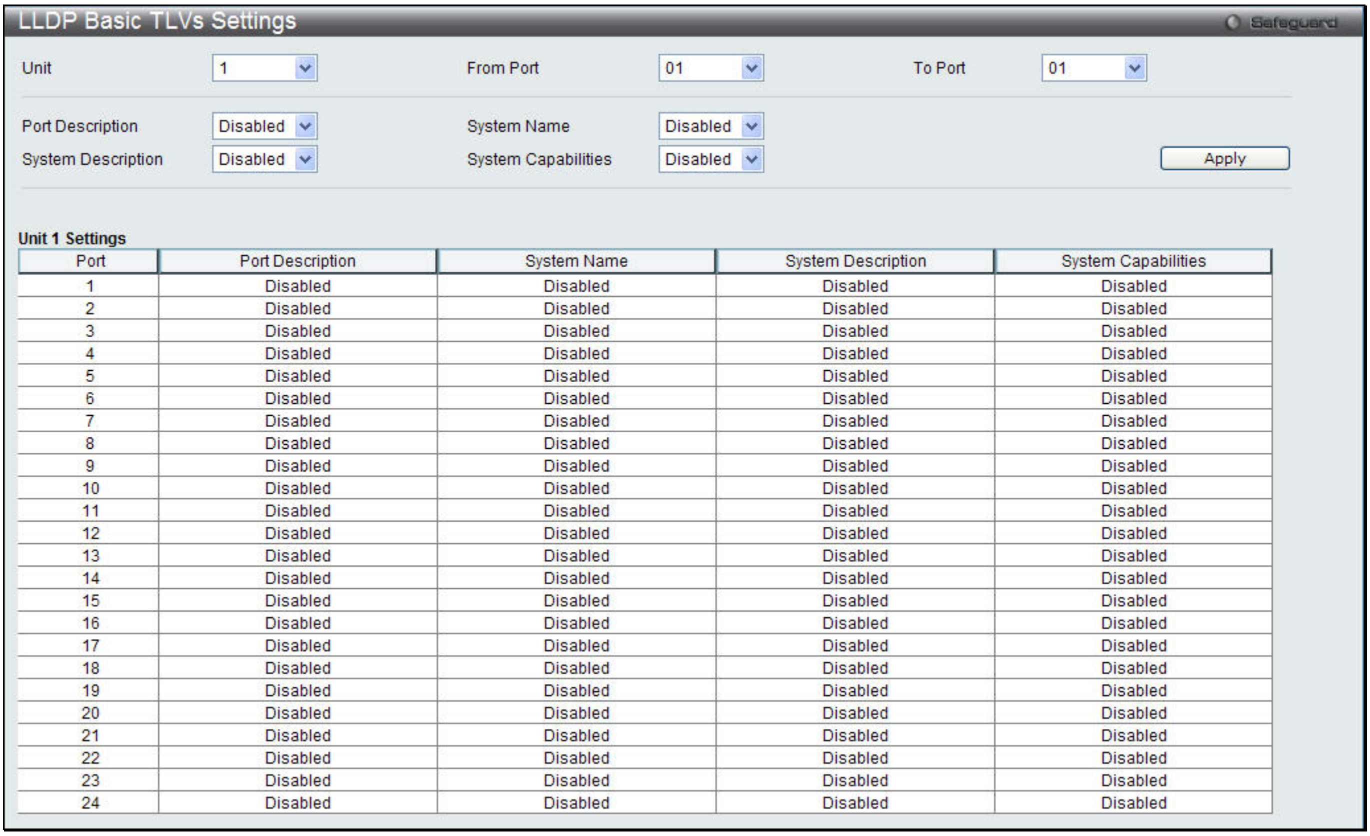
Parameter	Description
IPv4 / IPv6	Use the drop-down menu to select either IPv4 or IPv6.
Address	Enter the management IP address or the IP address of the entity you wish to advertise to. The IPv4 address is a management IP address, so the IP information will be sent with the frame.

Click the **Find** button to locate a specific entry based on the information entered.

LLDP Basic TLVs Settings

TLV stands for Type-length-value, which allows the specific sending information as a TLV element within LLDP packets. This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always included mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include Port Description, System Name, System Description and System Capability.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Basic TLVs Settings**, as show below:



LLDP Basic TLVs Settings

Unit: 1
From Port: 01
To Port: 01

Port Description: Disabled
System Name: Disabled
System Description: Disabled
System Capabilities: Disabled

Unit 1 Settings

Port	Port Description	System Name	System Description	System Capabilities
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled

Figure 4-94 LLDP Basic TLVs Settings window

The fields that can be configured are described below:

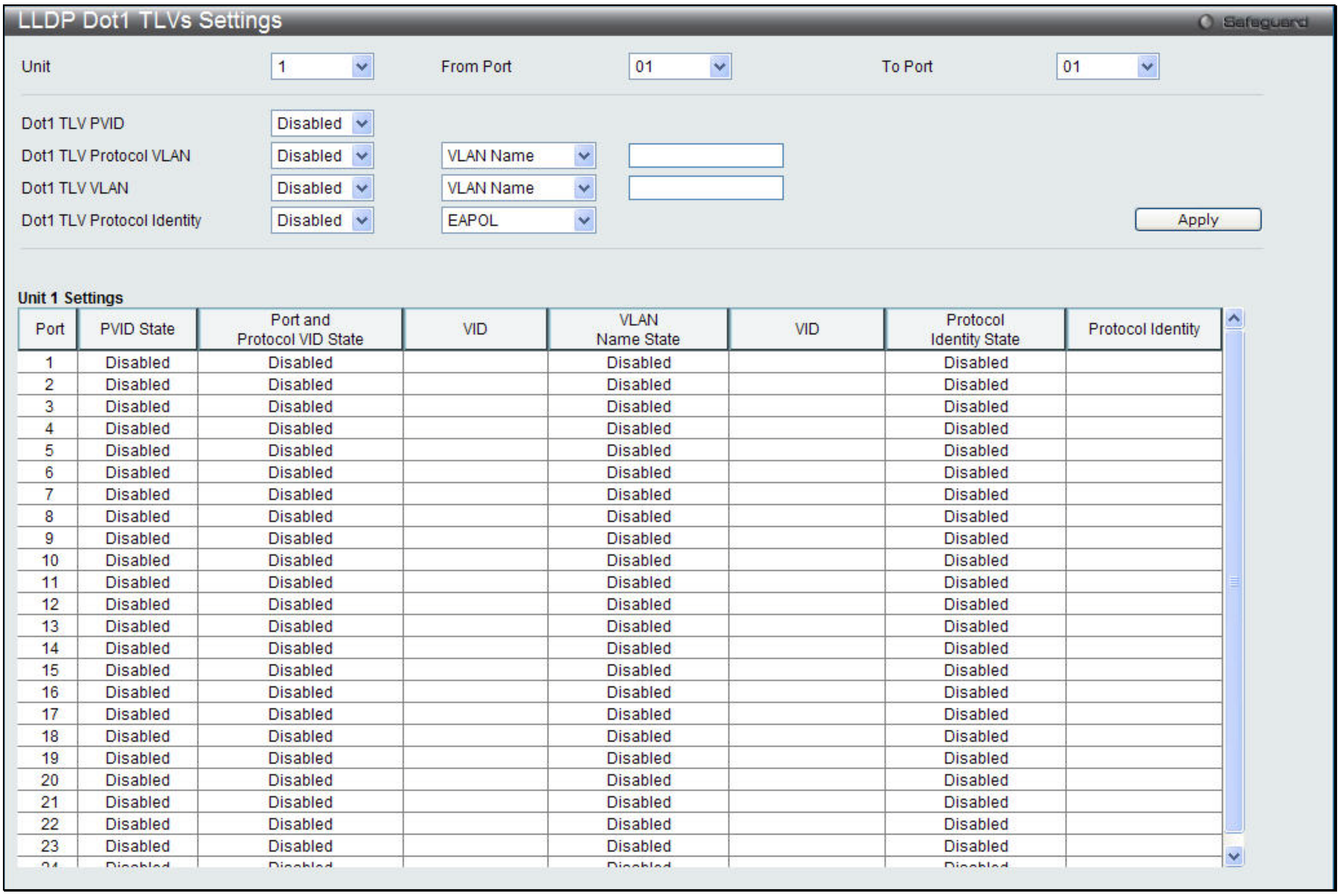
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the port range to use for this configuration.
Port Description	Use the drop-down menu to enable or disable the Port Description option.
System Name	Use the drop-down menu to enable or disable the System Name option.
System Description	Use the drop-down menu to enable or disable the System Description option.
System Capabilities	Use the drop-down menu to enable or disable the System Capabilities option.

Click the **Apply** button to accept the changes made.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Dot1 TLVs Settings**, as show below:



Unit: 1 From Port: 01 To Port: 01

Dot1 TLV PVID: Disabled

Dot1 TLV Protocol VLAN: Disabled VLAN Name

Dot1 TLV VLAN: Disabled VLAN Name

Dot1 TLV Protocol Identity: Disabled EAPOL

Unit 1 Settings

Port	PVID State	Port and Protocol VID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
1	Disabled	Disabled		Disabled		Disabled	
2	Disabled	Disabled		Disabled		Disabled	
3	Disabled	Disabled		Disabled		Disabled	
4	Disabled	Disabled		Disabled		Disabled	
5	Disabled	Disabled		Disabled		Disabled	
6	Disabled	Disabled		Disabled		Disabled	
7	Disabled	Disabled		Disabled		Disabled	
8	Disabled	Disabled		Disabled		Disabled	
9	Disabled	Disabled		Disabled		Disabled	
10	Disabled	Disabled		Disabled		Disabled	
11	Disabled	Disabled		Disabled		Disabled	
12	Disabled	Disabled		Disabled		Disabled	
13	Disabled	Disabled		Disabled		Disabled	
14	Disabled	Disabled		Disabled		Disabled	
15	Disabled	Disabled		Disabled		Disabled	
16	Disabled	Disabled		Disabled		Disabled	
17	Disabled	Disabled		Disabled		Disabled	
18	Disabled	Disabled		Disabled		Disabled	
19	Disabled	Disabled		Disabled		Disabled	
20	Disabled	Disabled		Disabled		Disabled	
21	Disabled	Disabled		Disabled		Disabled	
22	Disabled	Disabled		Disabled		Disabled	
23	Disabled	Disabled		Disabled		Disabled	

Figure 4-95 LLDP Dot1 TLVs Settings window

The fields that can be configured are described below:

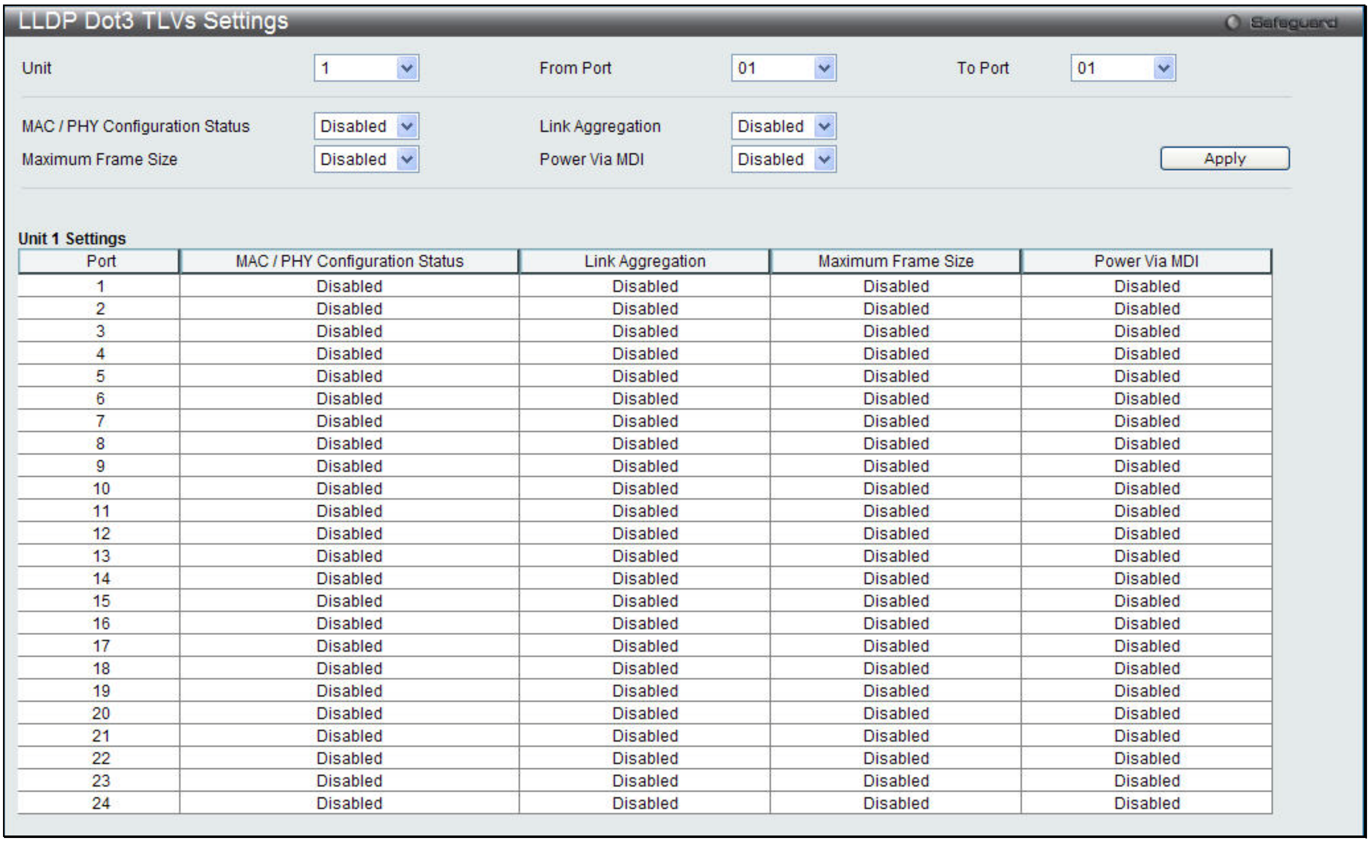
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Dot1 TLV PVID	Use the drop-down menu to enable or disable and configure the Dot1 TLV PVID option.
Dot1 TLV Protocol VLAN	Use the drop-down menu to enable or disable, and configure the Dot1 TLV Protocol VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV VLAN	Use the drop-down menu to enable or disable, and configure the Dot1 TLV VLAN option. After enabling this option to the user can select to use either **VLAN Name**, **VID List** or **All** in the next drop-down menu. After selecting this, the user can enter either the **VLAN Name** or **VID List** value in the space provided.
Dot1 TLV Protocol Identity	Use the drop-down menu to enable or disable, and configure the Dot1 TLV Protocol Identity option. After enabling this option the user can select to either use **EAPOL**, **LACP**, **GVRP**, **STP**, or **All**.

Click the **Apply** button to accept the changes made.

LLDP Dot3 TLVs Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Dot3 TLVs Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
MAC / PHY Configuration Status: Disabled
Link Aggregation: Disabled
Maximum Frame Size: Disabled
Power Via MDI: Disabled

Unit 1 Settings

Port	MAC / PHY Configuration Status	Link Aggregation	Maximum Frame Size	Power Via MDI
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled

Figure 4-96 LLDP Dot3 TLVs Settings window

The fields that can be configured are described below:

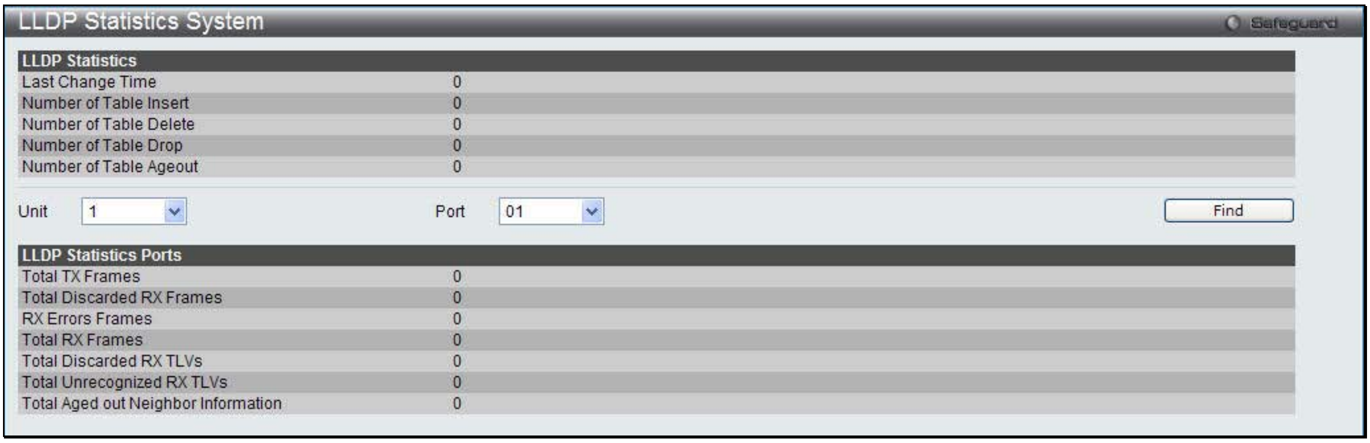
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
MAC / PHY Configuration Status	This TLV optional data type indicates that the LLDP agent should transmit the MAC/PHY configuration/status TLV. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is Disabled.
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is Disabled.
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is Disabled.
Power Via MDI	Use the drop down menu to enable or disable power via MDI. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

Click the **Apply** button to accept the changes made.

LLDP Statistic System

The LLDP Statistics System page allows you an overview of the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Statistic System**, as show below:



LLDP Statistics	
Last Change Time	0
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Ageout	0

Unit 1 Port 01

LLDP Statistics Ports	
Total TX Frames	0
Total Discarded RX Frames	0
RX Errors Frames	0
Total RX Frames	0
Total Discarded RX TLVs	0
Total Unrecognized RX TLVs	0
Total Aged out Neighbor Information	0

Figure 4-97 LLDP Statistics System window

The fields that can be configured are described below:

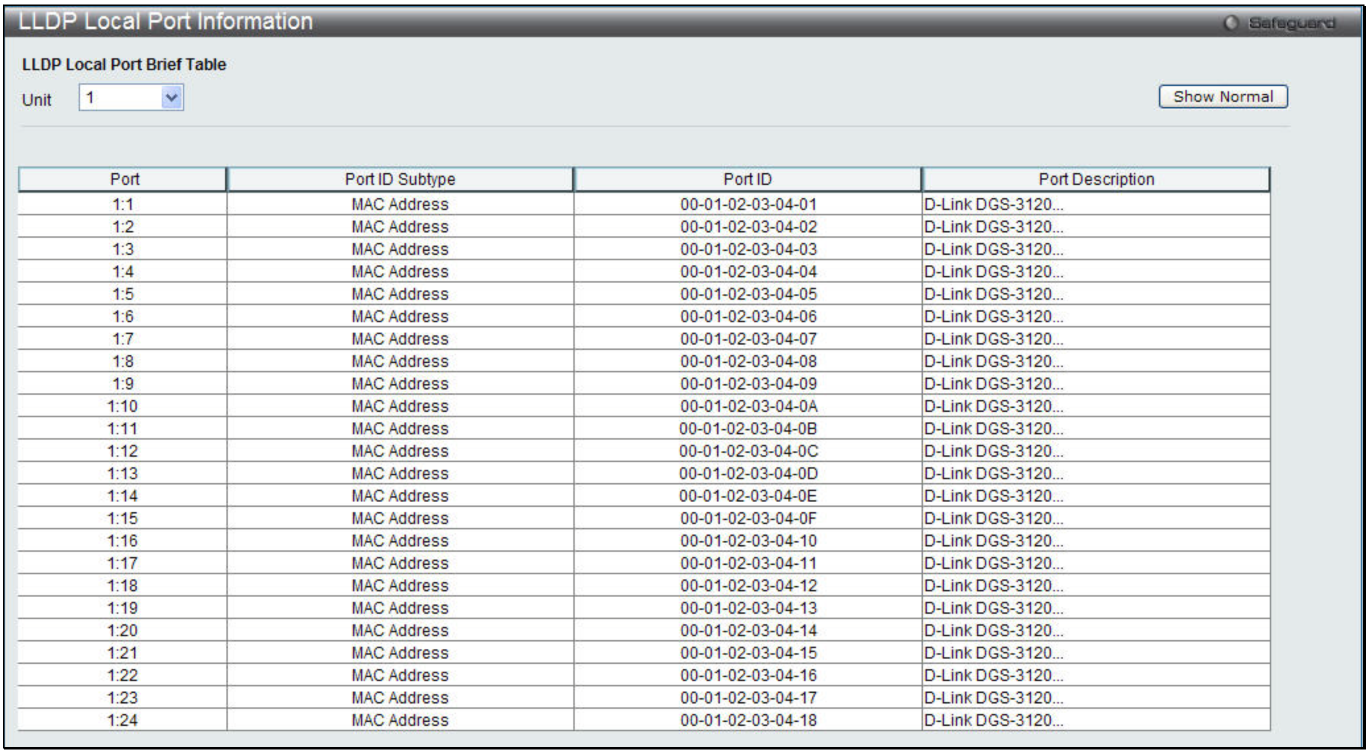
Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select a port.

Click the **Find** button to locate a specific entry based on the information entered.

LLDP Local Port Information

The LLDP Local Port Information page displays the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Local Port Information**, as show below:



LLDP Local Port Brief Table

Unit 1

Port	Port ID Subtype	Port ID	Port Description
1:1	MAC Address	00-01-02-03-04-01	D-Link DGS-3120...
1:2	MAC Address	00-01-02-03-04-02	D-Link DGS-3120...
1:3	MAC Address	00-01-02-03-04-03	D-Link DGS-3120...
1:4	MAC Address	00-01-02-03-04-04	D-Link DGS-3120...
1:5	MAC Address	00-01-02-03-04-05	D-Link DGS-3120...
1:6	MAC Address	00-01-02-03-04-06	D-Link DGS-3120...
1:7	MAC Address	00-01-02-03-04-07	D-Link DGS-3120...
1:8	MAC Address	00-01-02-03-04-08	D-Link DGS-3120...
1:9	MAC Address	00-01-02-03-04-09	D-Link DGS-3120...
1:10	MAC Address	00-01-02-03-04-0A	D-Link DGS-3120...
1:11	MAC Address	00-01-02-03-04-0B	D-Link DGS-3120...
1:12	MAC Address	00-01-02-03-04-0C	D-Link DGS-3120...
1:13	MAC Address	00-01-02-03-04-0D	D-Link DGS-3120...
1:14	MAC Address	00-01-02-03-04-0E	D-Link DGS-3120...
1:15	MAC Address	00-01-02-03-04-0F	D-Link DGS-3120...
1:16	MAC Address	00-01-02-03-04-10	D-Link DGS-3120...
1:17	MAC Address	00-01-02-03-04-11	D-Link DGS-3120...
1:18	MAC Address	00-01-02-03-04-12	D-Link DGS-3120...
1:19	MAC Address	00-01-02-03-04-13	D-Link DGS-3120...
1:20	MAC Address	00-01-02-03-04-14	D-Link DGS-3120...
1:21	MAC Address	00-01-02-03-04-15	D-Link DGS-3120...
1:22	MAC Address	00-01-02-03-04-16	D-Link DGS-3120...
1:23	MAC Address	00-01-02-03-04-17	D-Link DGS-3120...
1:24	MAC Address	00-01-02-03-04-18	D-Link DGS-3120...

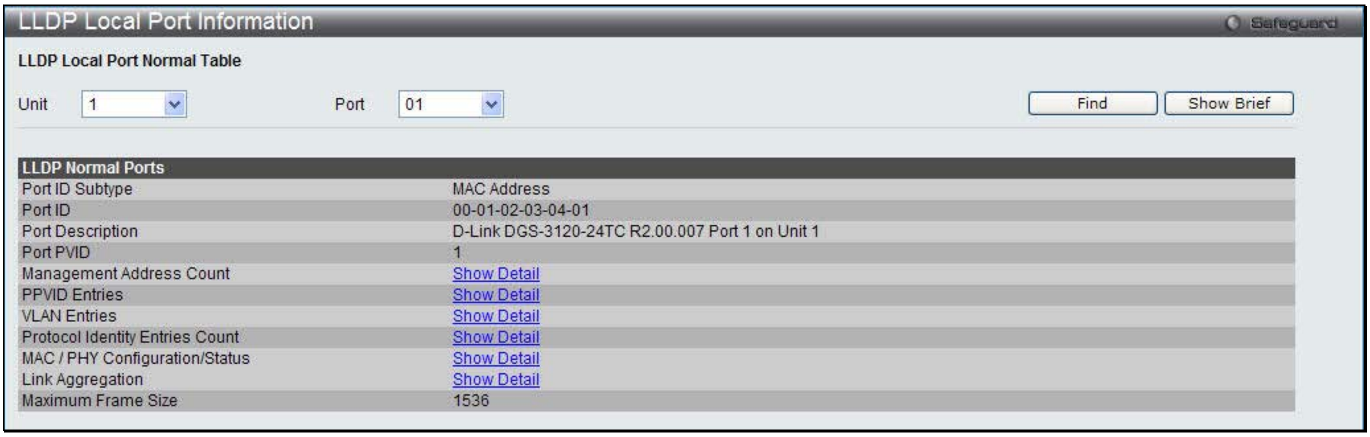
Figure 4-98 LLDP Local Port Information window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.

To view the normal LLDP Local Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:



LLDP Local Port Normal Table

LLDP Normal Ports	
Port ID Subtype	MAC Address
Port ID	00-01-02-03-04-01
Port Description	D-Link DGS-3120-24TC R2.00.007 Port 1 on Unit 1
Port PVID	1
Management Address Count	Show Detail
PPVID Entries	Show Detail
VLAN Entries	Show Detail
Protocol Identity Entries Count	Show Detail
MAC / PHY Configuration/Status	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536

Figure 4-99 LLDP Local Port Information – Show Normal window

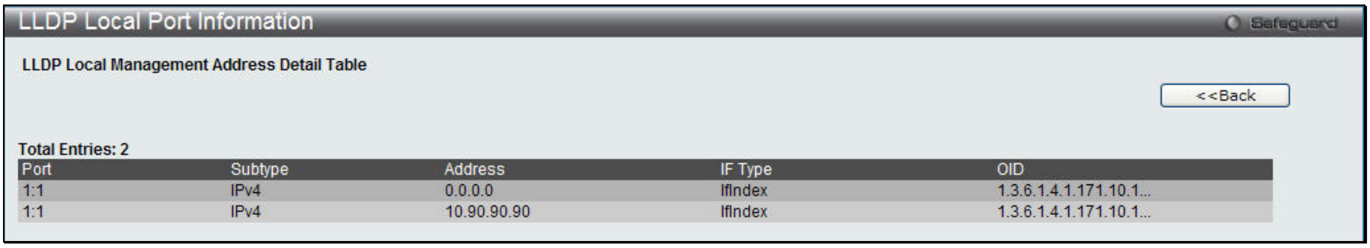
The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select a port.

Click the **Find** button to locate a specific entry based on the information entered.

To view more details about, for example, the **Management Address Count**, click on the Show Detail hyperlink.

To view the brief LLDP Local Port information page per port, click the **Show Brief** button.



LLDP Local Management Address Detail Table

Total Entries: 2

Port	Subtype	Address	IF Type	OID
1:1	IPv4	0.0.0.0	IfIndex	1.3.6.1.4.1.171.10.1...
1:1	IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.171.10.1...

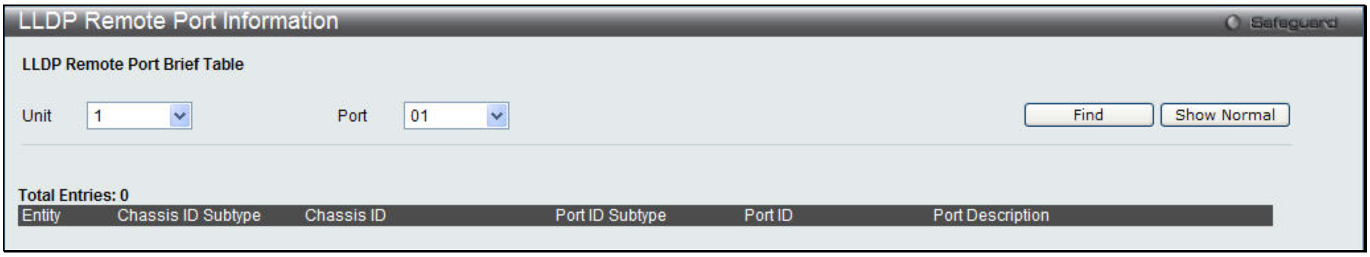
Figure 4-100 LLDP Local Port Information – Show Detail window

Click the **<<Back** button to return to the previous page.

LLDP Remote Port Information

This page displays port information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click **L2 Features > LLDP > LLDP > LLDP Remote Port Information**, as show below:



LLDP Remote Port Information

LLDP Remote Port Brief Table

Unit: 1
Port: 01

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description

Figure 4-101 LLDP Remote Port Information window

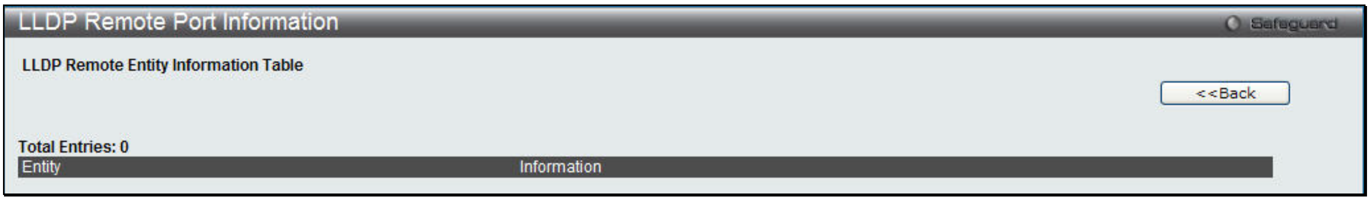
The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select a port.

Click the **Find** button to locate a specific entry based on the information entered.

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:



LLDP Remote Port Information

LLDP Remote Entity Information Table

Total Entries: 0

Entity	Information

Figure 4-102 LLDP Remote Port Information – Show Normal window

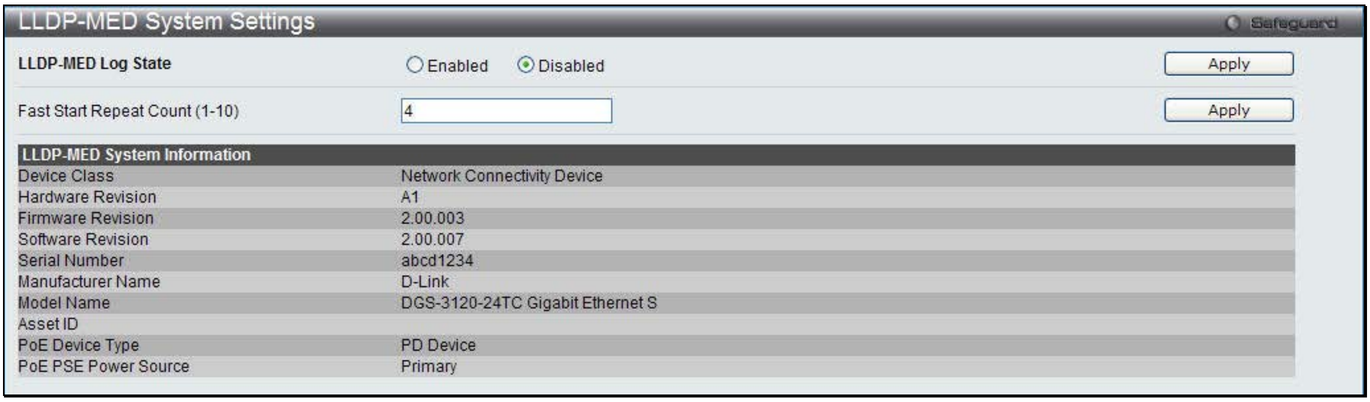
Click the **<<Back** button to return to the previous page.

LLDP-MED

LLDP-MED System Settings

This window is used to configure the LLDP-MED log state and the fast start repeat count, and display the LLDP-MED system information.

To view the following window, click **L2 Features > LLDP > LLDP-MED > LLDP-MED System Settings**, as show below:



LLDP-MED System Settings

LLDP-MED Log State ○ Enabled ● Disabled

Fast Start Repeat Count (1-10): 4

LLDP-MED System Information	
Device Class	Network Connectivity Device
Hardware Revision	A1
Firmware Revision	2.00.003
Software Revision	2.00.007
Serial Number	abcd1234
Manufacturer Name	D-Link
Model Name	DGS-3120-24TC Gigabit Ethernet S
Asset ID	
PoE Device Type	PD Device
PoE PSE Power Source	Primary

Figure 4-103 LLDP-MED System Settings window

The fields that can be configured are described below:

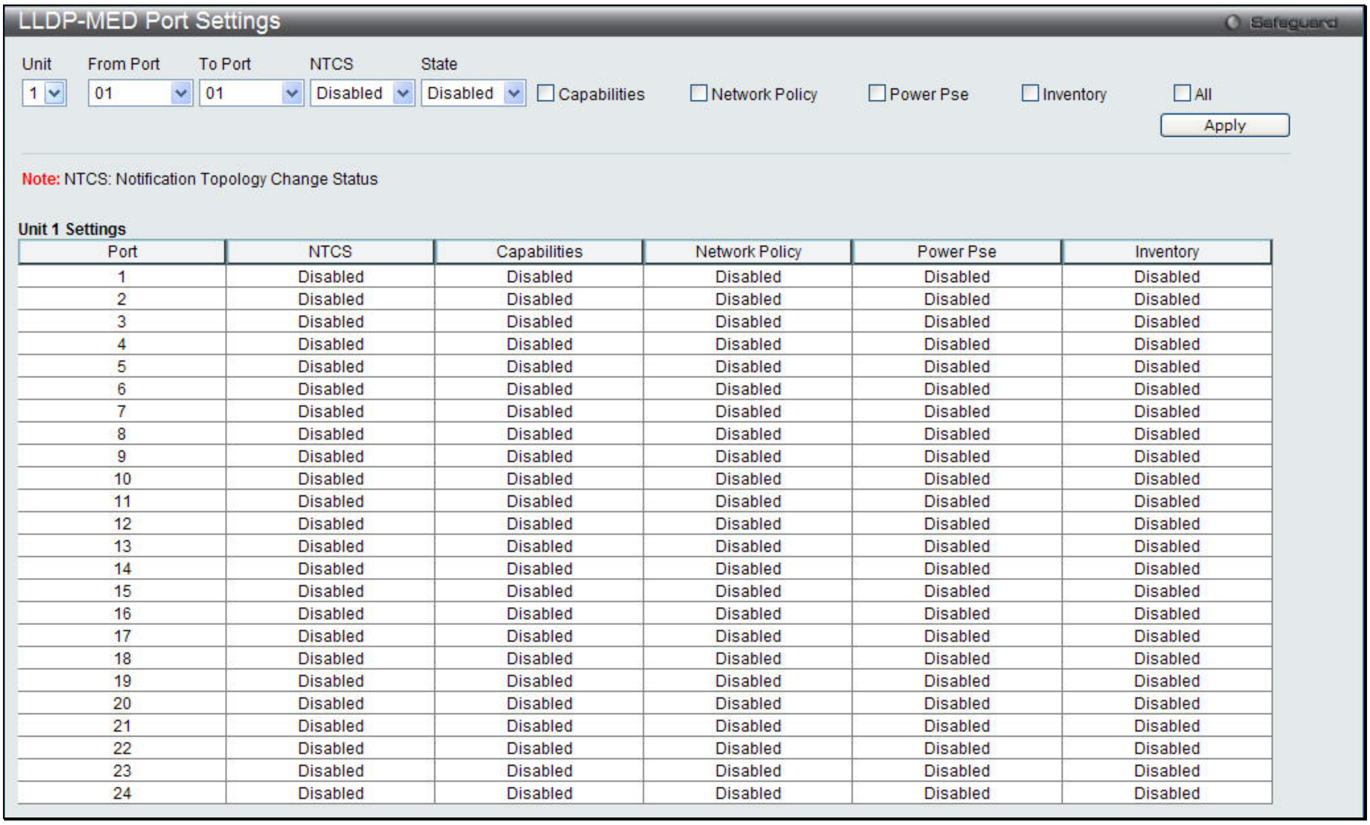
Parameter	Description
LLDP-MED Log State	Click to enable or disable the log state of LLDP-MED events.
Fast Start Repeat Count (1-10)	Enter a value between 1 and 10 for the fast start repeat count. When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, then the application layer shall start the fast start mechanism and set the 'medFastStart' timer to 'medFastStartRepeatCount' times 1. The default value is 4.

Click the **Apply** button to accept the changes made for each individual section.

LLDP-MED Port Settings

This window is used to enable or disable transmitting LLDP-MED TLVs.

To view the following window, click **L2 Features > LLDP > LLDP-MED > LLDP-MED Port Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
NTCS: Disabled
State: Disabled

Note: NTCS: Notification Topology Change Status

Unit 1 Settings

Port	NTCS	Capabilities	Network Policy	Power Pse	Inventory
1	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled	Disabled

Figure 4-104 LLDP-MED Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the port range to use for this configuration.
Port Description	Use the drop-down menu to enable or disable the Port Description option.
NTCS	Use the drop-down menu to enable or disable Notification Topology Change Status.
State	Use the drop-down menu to enable or disable transmit LLDP-MED TLVs, and tick the check boxes of the TLV types that the LLDP agent should transmit. TLV types are

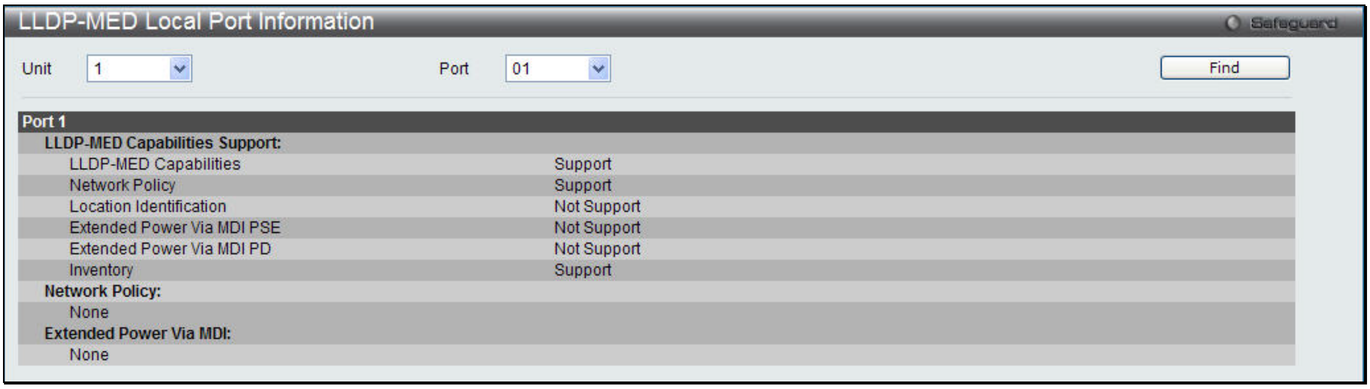
	Capabilities, **Network Policy**, and **Inventory**. Tick the **All** check box to select all TLV types.

Click the **Apply** button to accept the changes made.

LLDP-MED Local Port Information

This window displays the per-port information currently available for populating outbound LLDP-MED advertisements.

To view the following window, click **L2 Features > LLDP > LLDP-MED > LLDP-MED Local Port Information**, as show below:



Unit 1 Port 01

Port 1	
LLDP-MED Capabilities Support:	
LLDP-MED Capabilities	Support
Network Policy	Support
Location Identification	Not Support
Extended Power Via MDI PSE	Not Support
Extended Power Via MDI PD	Not Support
Inventory	Support
Network Policy:	
None	
Extended Power Via MDI:	
None	

Figure 4-105 LLDP-MED Local Port Information window

The fields that can be configured are described below:

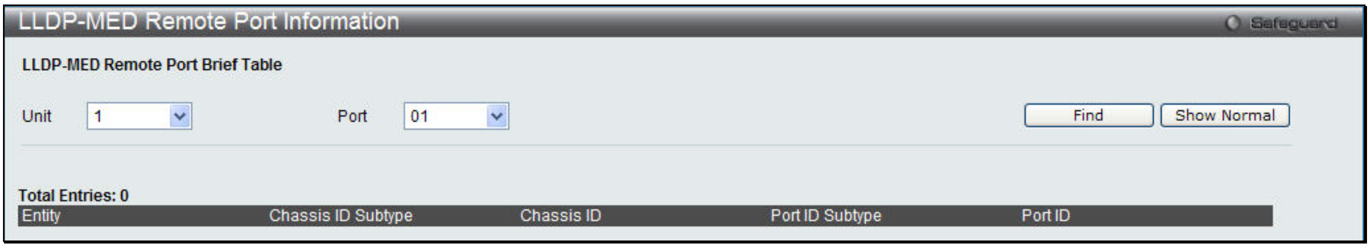
Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select a port.

Click the **Find** button to locate a specific entry based on the information entered.

LLDP-MED Remote Port Information

This window displays the information learned from the neighbor parameters.

To view the following window, click **L2 Features > LLDP > LLDP-MED > LLDP-MED Remote Port Information**, as show below:



LLDP-MED Remote Port Brief Table

Unit 1 Port 01

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID

Figure 4-106 LLDP-MED Remote Port Information window

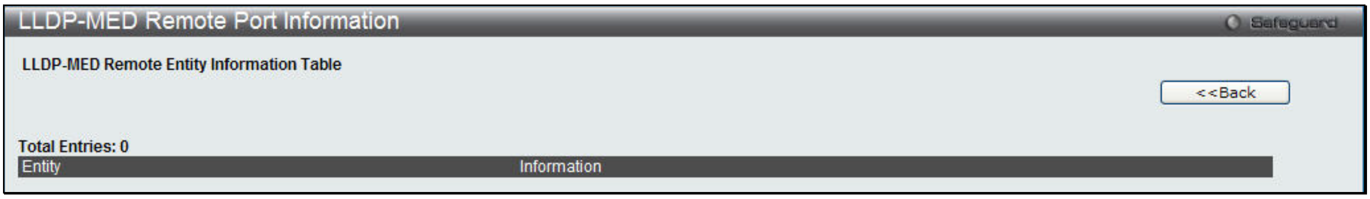
The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select a port.

Click the **Find** button to locate a specific entry based on the information entered.

To view the normal LLDP Remote Port information page per port, click the **Show Normal** button.

After clicking the **Show Normal** button, the following page will appear:



LLDP-MED Remote Port Information

LLDP-MED Remote Entity Information Table

Total Entries: 0

Entity	Information

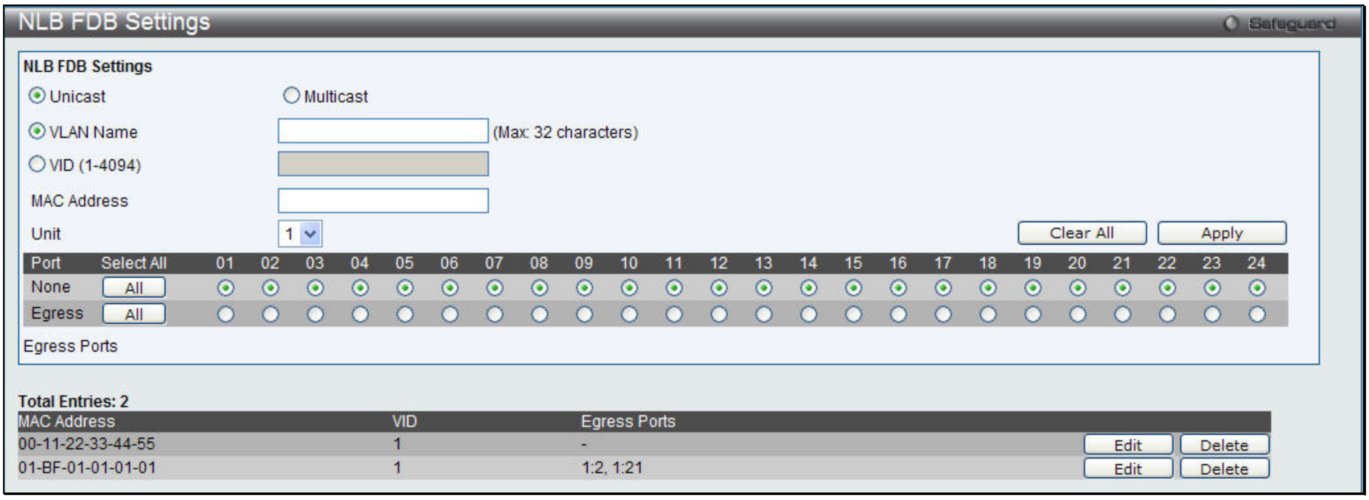
Figure 4-107 LLDP-MED Remote Port Information – Show Normal window

Click the **<<Back** button to return to the previous page.

NLB FDB Settings

The Switch supports Network Load Balancing (NLB). This is a MAC forwarding control for supporting the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. In multicast mode, the client uses a multicast MAC address as the destination MAC to reach the server. Regardless of the mode, the destination MAC is the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. The NLB multicast FDB entry will be mutually exclusive with the L2 multicast entry.

To view this window, click **L2 Features > NLB FDB Settings**, as shown below.



NLB FDB Settings

● Unicast ○ Multicast

● VLAN Name (Max: 32 characters)

○ VID (1-4094)

MAC Address

Unit 1

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Egress	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Egress Ports

Total Entries: 2

MAC Address	VID	Egress Ports	
00-11-22-33-44-55	1	-	Edit Delete
01-BF-01-01-01-01	1	1:2, 1:21	Edit Delete

Figure 4-108 NLB FDB Settings window

The fields that can be configured are described below:

Parameter	Description
Unicast	Click to create NLB unicast FDB entry.
Multicast	Click to NLB multicast FDB entry.
VLAN Name	Click the radio button and enter the VLAN of the NLB multicast FDB entry to be created.
VID (1-4094)	Click the radio button and enter the VLAN by the VLAN ID.
MAC Address	Enter the MAC address of the NLB multicast FDB entry to be created.
Unit	Select the unit you wish to configure.
Ports	Click the ports to be configured. Click the **All** button to select all ports.

Click the **Apply** button to accept the changes made.

Click the **Clear All** button to remove all the entered information in the fields.

Click the **Edit** button to update the information of the corresponding entry.

Click the **Delete** button to delete the corresponding entry.

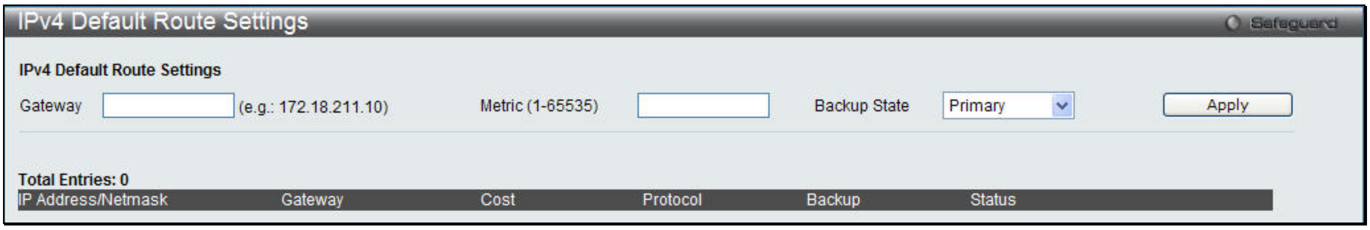
Chapter 5 L3 Features

IPv4 Default Route Settings (SI Mode Only)
IPv4 Static/Default Route Settings (EI Mode Only)
IPv4 Route Table
IPv6 Static/Default Route Settings (EI Mode Only)
IPv6 Route Table (EI Mode Only)
IP Forwarding Table

IPv4 Default Route Settings (SI Mode Only)

Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

To view the following window, click **L3 Features > IPv4 Default Route Settings**, as show below:



IPv4 Default Route Settings

Gateway (e.g.: 172.18.211.10) Metric (1-65535) Backup State Primary

Total Entries: 0

IP Address/Netmask	Gateway	Cost	Protocol	Backup	Status

Figure 5-1 IPv4 Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
Gateway	This field allows the entry of a Gateway IP Address to be applied to the corresponding gateway of the IP address.
Metric (1-65535)	Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.
Backup State	Specifies the backup state of the default route created. Option to choose from are **Primary** and **Backup**.

Click the **Apply** button to accept the changes made.

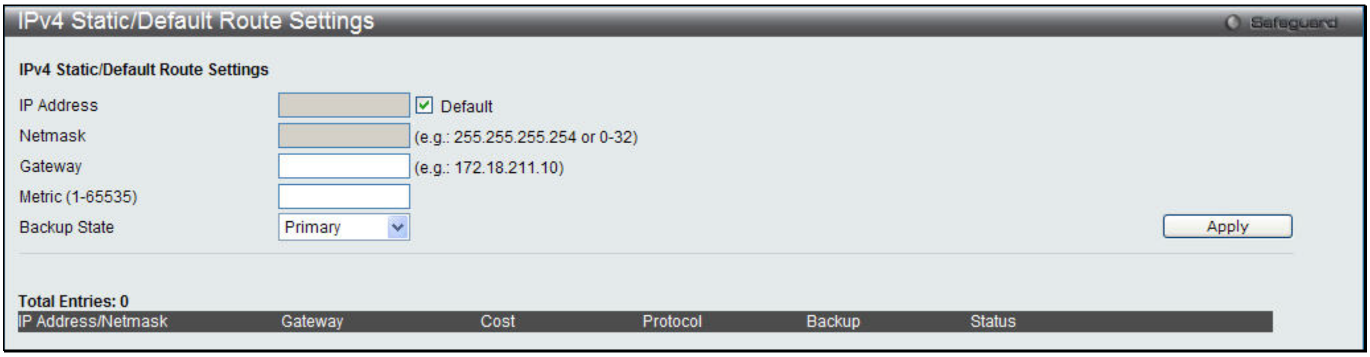
IPv4 Static/Default Route Settings (EI Mode Only)

The Switch supports static routing for IPv4 formatted addressing. Users can create up to 512 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP response will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

To view the following window, click **L3 Features > IPv4 Static/Default Route Settings**, as show below:


IPv4 Static/Default Route Settings
Safeguard
IPv4 Static/Default Route Settings
IP Address
☑ Default
Netmask
(e.g.: 255.255.255.254 or 0-32)
Gateway
(e.g.: 172.18.211.10)
Metric (1-65535)
Backup State
Primary
Apply

Total Entries: 0

IP Address/Netmask	Gateway	Cost	Protocol	Backup	Status

Figure 5-2 IPv4 Static/Default Route Settings window

The fields that can be configured are described below:

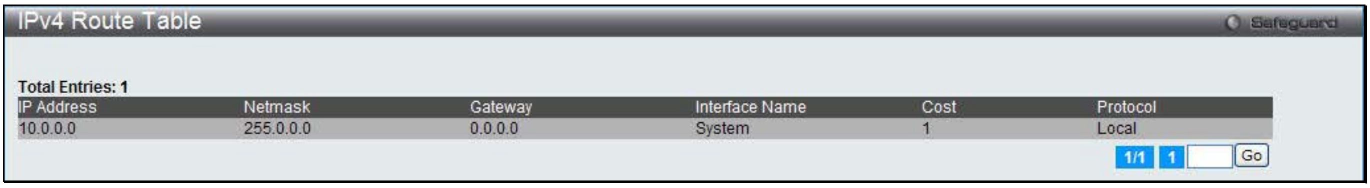
Parameter	Description
IP Address	This field allows the entry of an IPv4 address to be assigned to the static route. Tick the **Default** check box to assign to the default route.
Netmask	This field allows the entry of a subnet mask to be applied to the corresponding subnet mask of the IP address.
Gateway	This field allows the entry of a Gateway IP Address to be applied to the corresponding gateway of the IP address.
Metric (1-65535)	Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.

Click the **Apply** button to accept the changes made.

IPv4 Route Table

The IP routing table stores all the external routes information of the Switch. This window is used to display all the external route information on the switch.

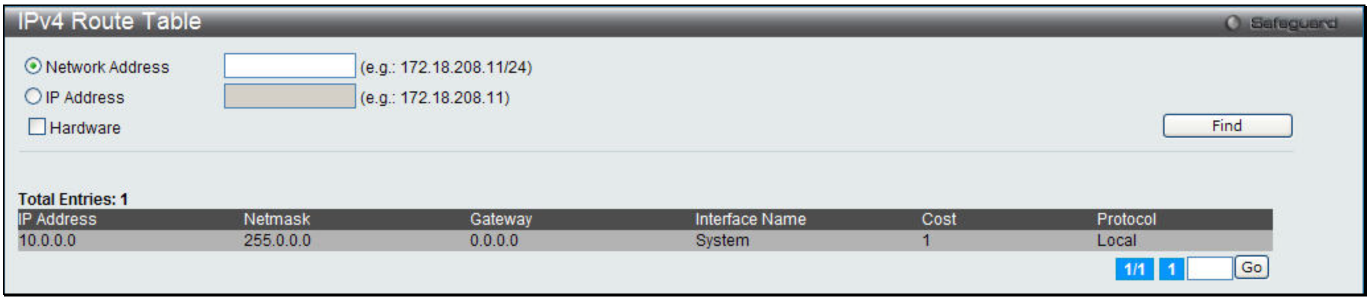
To view the following window, click **L3 Features > IPv4 Route Table**, as show below:


IPv4 Route Table
Safeguard
1/1
1
Go

Total Entries: 1

IP Address	Netmask	Gateway	Interface Name	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

Figure 5-3 IPv4 Route Table window (SI Mode Only)


IPv4 Route Table
Safeguard
● Network Address
(e.g.: 172.18.208.11/24)
○ IP Address
(e.g.: 172.18.208.11)
☐ Hardware
Find
1/1
1
Go

Total Entries: 1

IP Address	Netmask	Gateway	Interface Name	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

Figure 5-4 IPv4 Route Table window (EI Mode Only)

The fields that can be configured are described below: **(EI Mode Only)**

Parameter	Description
Network Address	Click the radio button and enter the destination network address of the route to be displayed.
IP Address	Click the radio button and enter the destination IP address of the route to be displayed. The longest prefix matched route will be displayed.
Hardware	Tick the check box to display only the routes that have been written into the chip.

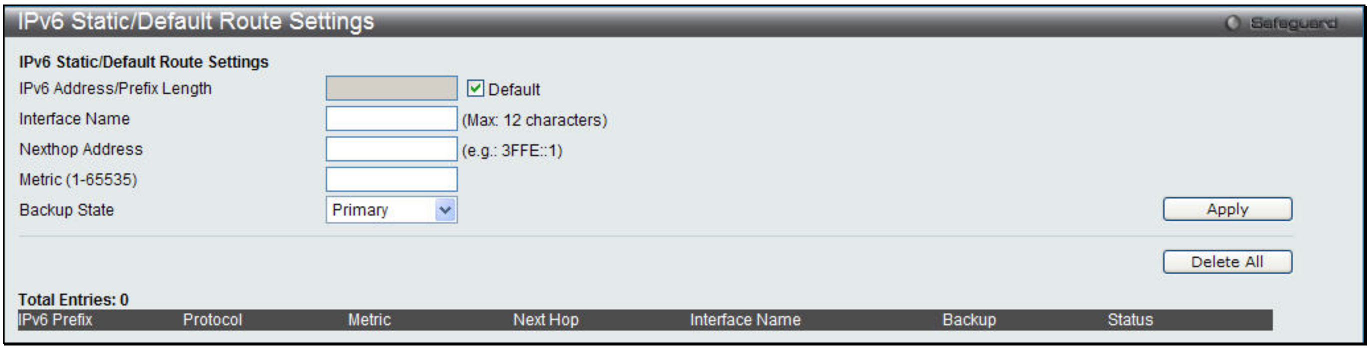
Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IPv6 Static/Default Route Settings (EI Mode Only)

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

To view the following window, click **L3 Features > IPv6 Static/Default Route Settings**, as show below:



IPv6 Static/Default Route Settings

IPv6 Address/Prefix Length		☑ Default
Interface Name		(Max: 12 characters)
Nexthop Address		(e.g.: 3FFE::1)
Metric (1-65535)		
Backup State	Primary	

Total Entries: 0

IPv6 Prefix	Protocol	Metric	Next Hop	Interface Name	Backup	Status

Figure 5-5 IPv6 Static/Default Route Settings window

The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	This field allows the entry of an IPv6 address to be assigned to the static route. Tick the **Default** check box to assign to the default route.
Interface Name	The IP Interface where the static IPv6 route is created.
Nexthop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1 and 65535.
Backup State	Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, the switch will try the backup routes according to the order learnt by the routing table until route success. This field represents the backup state for the IPv6 configured. This field may be Primary or Backup.

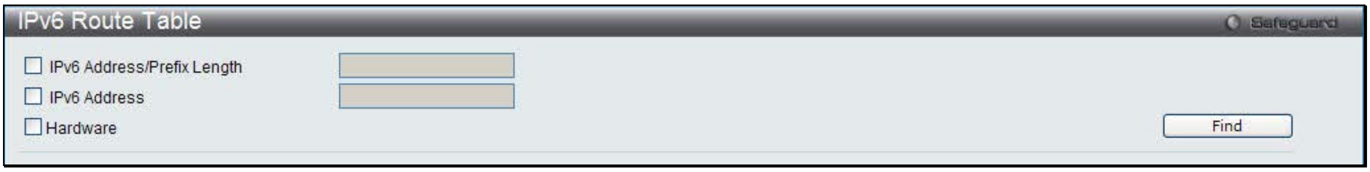
Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

IPv6 Route Table (EI Mode Only)

This window is used to Display the current IPv6 routing table or specified route entries.

To view the following window, click **L3 Features > IPv6 Route Table**, as show below:



IPv6 Route Table

☐ IPv6 Address/Prefix Length
☐ IPv6 Address
☐ Hardware

Figure 5-6 IPv6 Route Table window

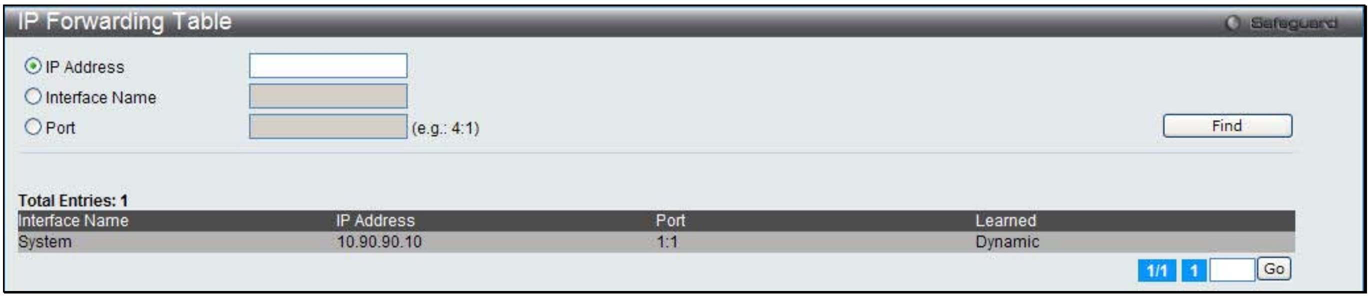
The fields that can be configured are described below:

Parameter	Description
IPv6 Address/Prefix Length	Tick the check box and enter a 128-bit length IPv6 address.
IPv6 Address	Tick the check box and enter the destination IP address of the route to be displayed.
Hardware	Tick the check box to display only the routes that have been written into the chip.

Click the **Find** button to locate a specific entry based on the information entered.

IP Forwarding Table

The IP forwarding table stores all the direct connected IP information. On this page the user can view all the direct connected IP information. To view the following window, click **L3 Features > IP Forwarding Table**, as show below:



IP Forwarding Table

● IP Address
○ Interface Name
○ Port (e.g.: 4:1)

Total Entries: 1

Interface Name	IP Address	Port	Learned
System	10.90.90.10	1:1	Dynamic

Figure 5-7 IP Forwarding Table

The fields that can be configured are described below:

Parameter	Description
IP Address	Click the radio button and enter the IP address.
Interface Name	Click the radio button and enter the interface name.
Port	Click the radio button and enter the port.

Click the **Find** button to locate a specific entry based on the information entered.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Chapter 6 QoS

802.1p Settings
Bandwidth Control
Traffic Control Settings
DSCP
HOL Blocking Prevention
Scheduling Settings

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements basic 802.1P priority queuing.

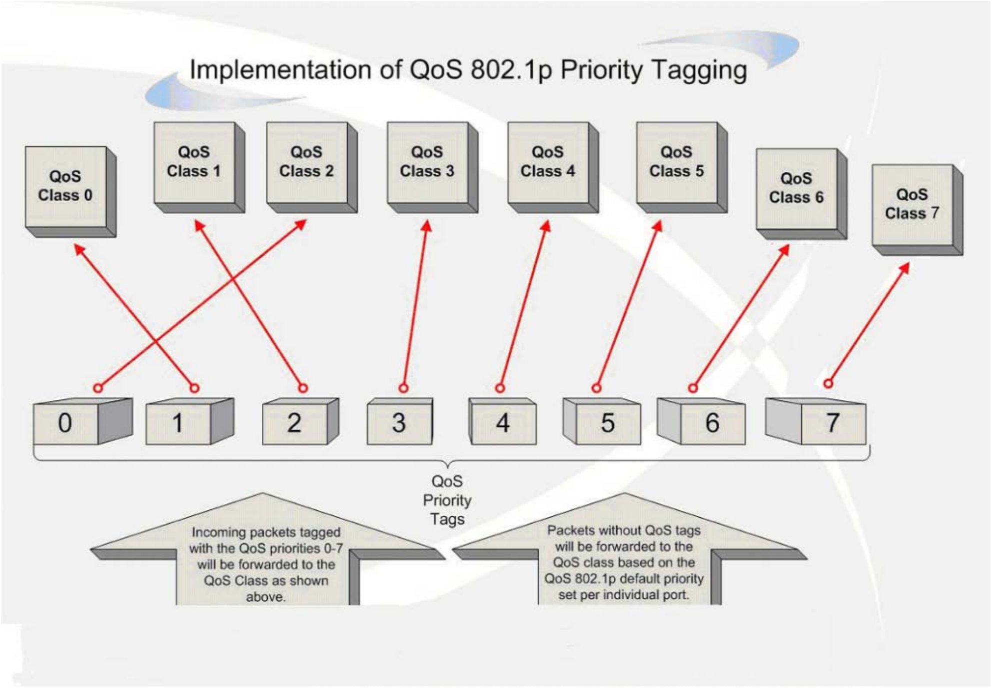

Implementation of QoS 802.1p Priority Tagging
QoS Class 0
QoS Class 1
QoS Class 2
QoS Class 3
QoS Class 4
QoS Class 5
QoS Class 6
QoS Class 7
0
1
2
3
4
5
6
7
QoS Priority Tags
Incoming packets tagged with the QoS priorities 0-7 will be forwarded to the QoS Class as shown above.
Packets without QoS tags will be forwarded to the QoS class based on the QoS 802.1p default priority set per individual port.

Figure 6-1 Mapping QoS on the Switch

The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let’s say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch supports 802.1p priority queuing. The Switch has eight priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of eight CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the Switch has eight configurable priority queues (and eight Classes of Service) for each port on the Switch.

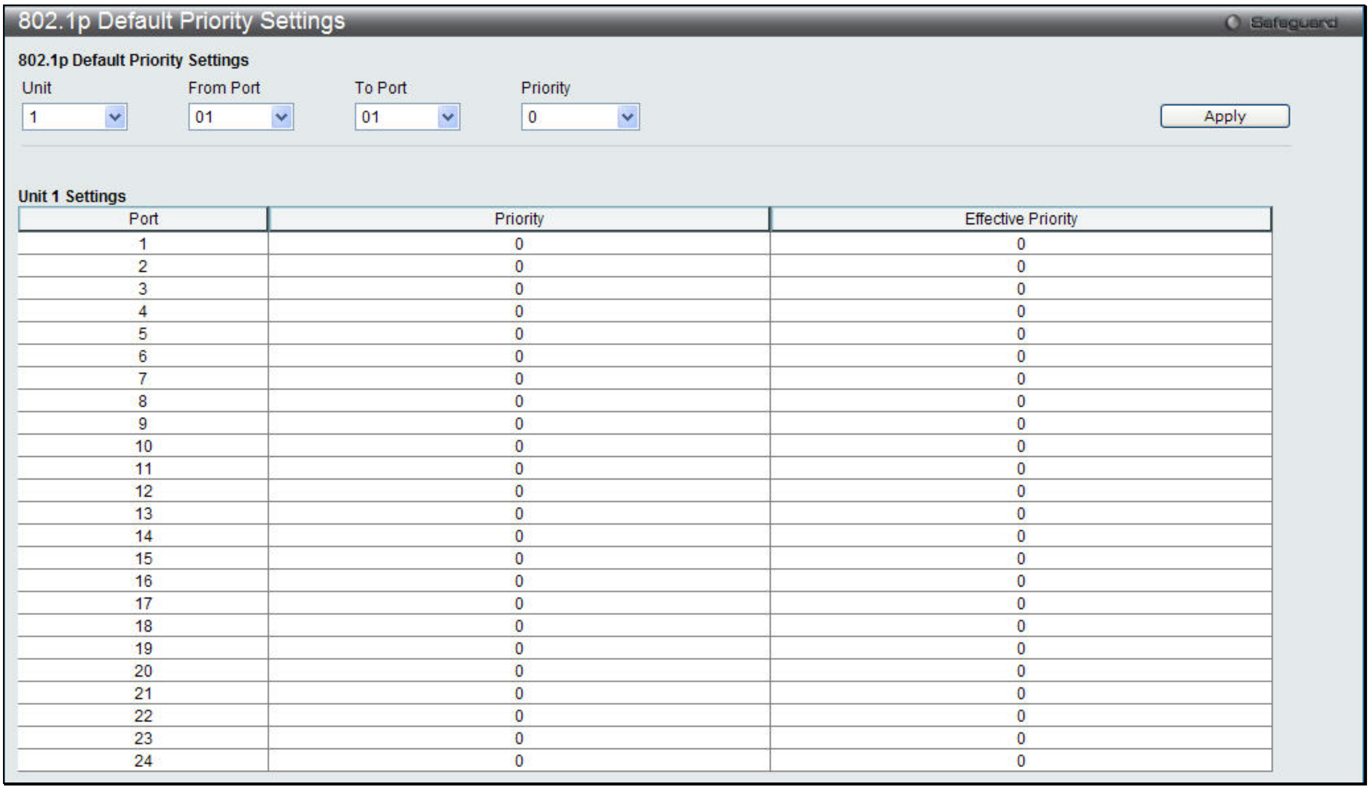
NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the eight classes of service that may be used and configured by the administrator.

802.1p Settings

802.1p Default Priority Settings

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. This page allows the user to assign a default 802.1p priority to any given port on the switch that will insert the 802.1p priority tag to untagged packets received. The priority and effective priority tags are numbered from *0*, the lowest priority, to *7*, the highest priority. The effective priority indicates the actual priority assigned by RADIUS. If the RADIUS assigned value exceeds the specified limit, the value will be set at the default priority. For example, if the RADIUS assigns a limit of 8 and the default priority is 0, the effective priority will be 0.

To view the following window, click **QoS > 802.1p Settings > 802.1p Default Priority Settings**, as show below:



802.1p Default Priority Settings

802.1p Default Priority Settings

Unit: 1
From Port: 01
To Port: 01
Priority: 0

Unit 1 Settings

Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0

Figure 6-2 Default Priority Settings window

The fields that can be configured are described below:

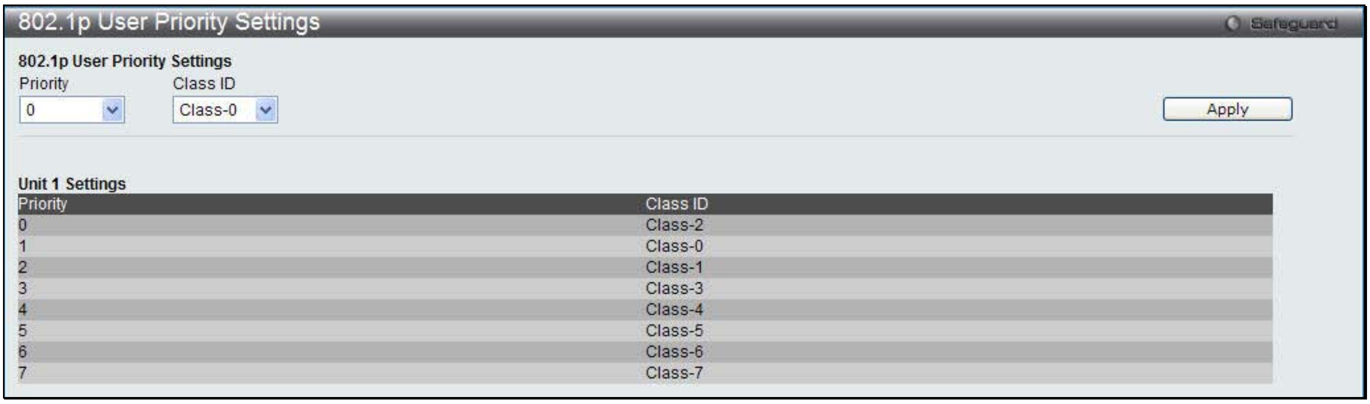
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select the starting and ending ports to use.
Priority	Use the drop-down menu to select a value from *0* to *7*.

Click the **Apply** button to accept the changes made.

802.1p User Priority Settings

The Switch allows the assignment of a class of service to each of the 802.1p priorities.

To view the following window, click **QoS > 802.1p Settings > 802.1p User Priority Settings**, as show below:



802.1p User Priority Settings

802.1p User Priority Settings

Priority: 0
Class ID: Class-0

Unit 1 Settings

Priority	Class ID
0	Class-2
1	Class-0
2	Class-1
3	Class-3
4	Class-4
5	Class-5
6	Class-6
7	Class-7

Figure 6-3 802.1p User Priority Settings window

Once a priority has been assigned to the port groups on the Switch, then a Class may be assigned to each of the eight levels of 802.1p priorities using the drop-down menus on this window. User priority mapping is not only for the default priority configured in the last page, but also for all the incoming tagged packets with 802.1p tag.

Click the **Apply** button to accept the changes made.

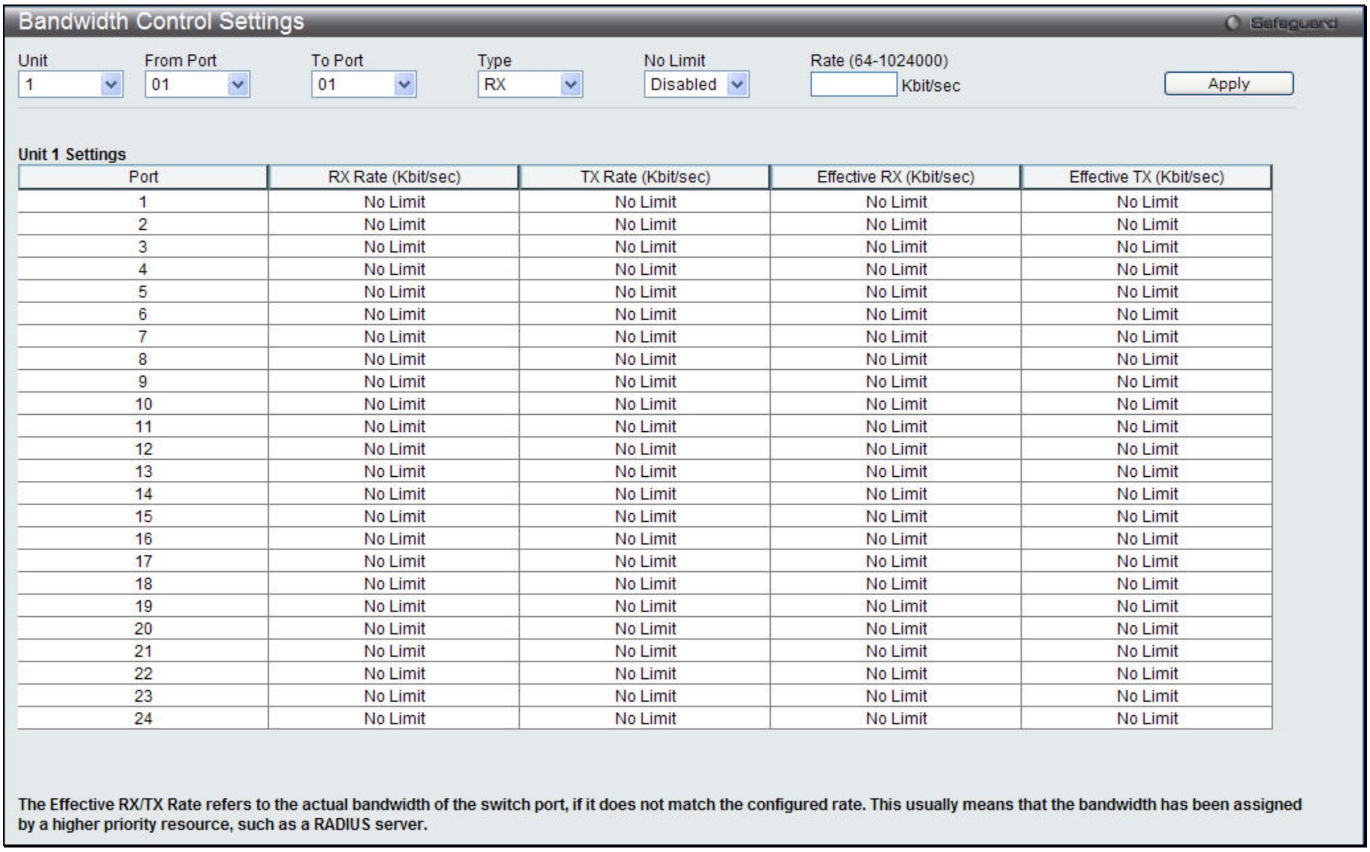
Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

Bandwidth Control Settings

The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

To view the following window, click **QoS > Bandwidth Control > Bandwidth Control Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
Type: RX
No Limit: Disabled
Rate (64-1024000): Kbit/sec

Unit 1 Settings

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit
11	No Limit	No Limit	No Limit	No Limit
12	No Limit	No Limit	No Limit	No Limit
13	No Limit	No Limit	No Limit	No Limit
14	No Limit	No Limit	No Limit	No Limit
15	No Limit	No Limit	No Limit	No Limit
16	No Limit	No Limit	No Limit	No Limit
17	No Limit	No Limit	No Limit	No Limit
18	No Limit	No Limit	No Limit	No Limit
19	No Limit	No Limit	No Limit	No Limit
20	No Limit	No Limit	No Limit	No Limit
21	No Limit	No Limit	No Limit	No Limit
22	No Limit	No Limit	No Limit	No Limit
23	No Limit	No Limit	No Limit	No Limit
24	No Limit	No Limit	No Limit	No Limit

The Effective RX/TX Rate refers to the actual bandwidth of the switch port, if it does not match the configured rate. This usually means that the bandwidth has been assigned by a higher priority resource, such as a RADIUS server.

Figure 6-4 Bandwidth Control Settings window

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Type	This drop-down menu allows a selection between **RX** (receive), **TX** (transmit), and **Both**. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows the user to specify that the selected port will have no bandwidth limit or not. **NOTE:** If the configured number is larger than the port speed, it means no bandwidth limit.
Rate (64-1024000)	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between *64* and *1024000* Kbits per second.

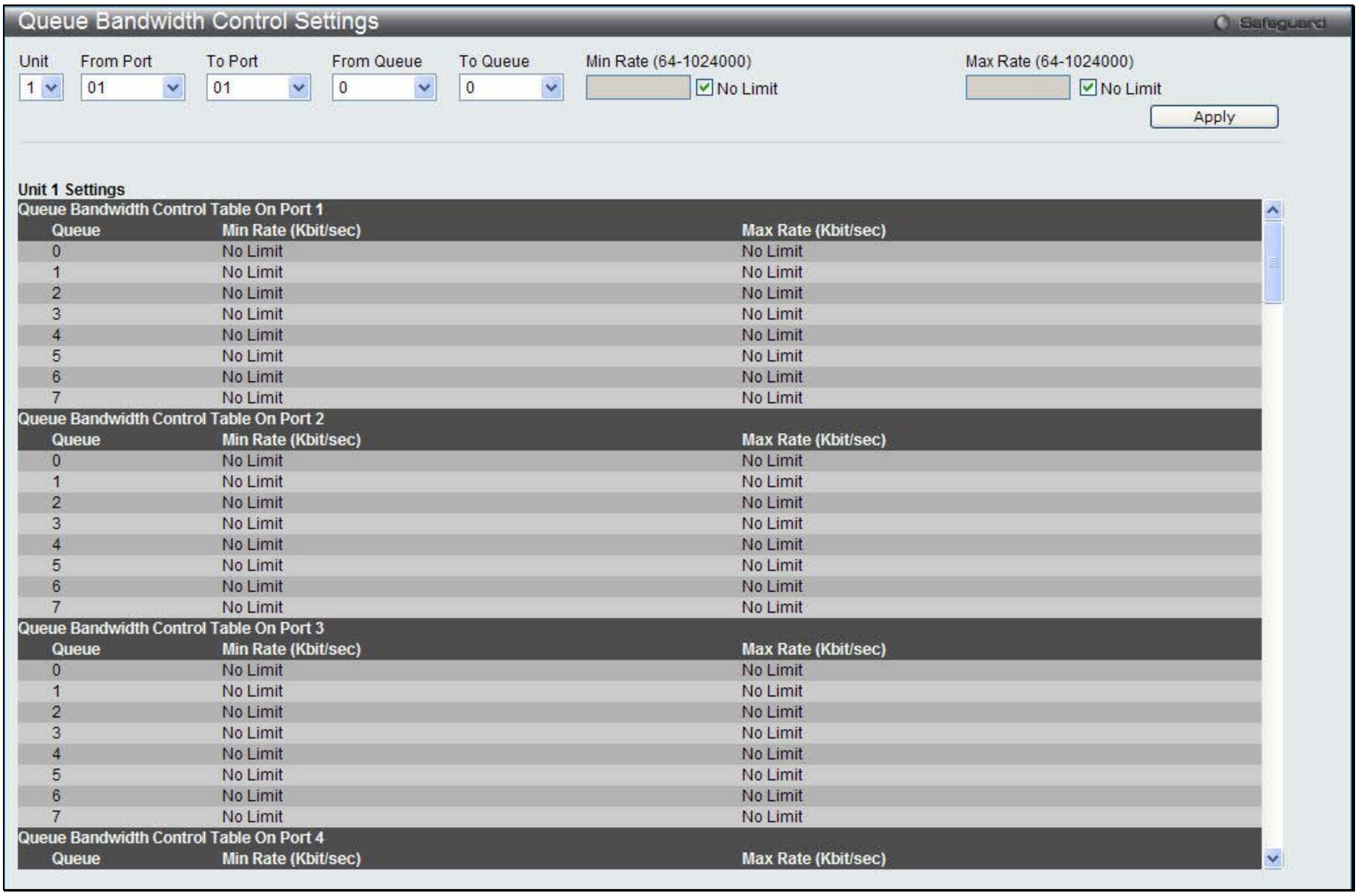
Effective RX	If a RADIUS server has assigned the RX bandwidth, then it will be the effective RX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple RX bandwidths assigned if there are multiple users attached to this specific port. The final RX bandwidth will be the largest one among these multiple RX bandwidths.
Effective TX	If a RADIUS server has assigned the TX bandwidth, then it will be the effective TX bandwidth. The authentication with the RADIUS sever can be per port or per user. For per user authentication, there may be multiple TX bandwidths assigned if there are multiple users attached to this specific port. The final TX bandwidth will be the largest one among these multiple TX bandwidths.

Click the **Apply** button to accept the changes made.

Queue Bandwidth Control Settings

To view this window, click **QoS > Bandwidth Control > Queue Bandwidth Control Settings**, as shown below.

To view the following window, click **QoS > Bandwidth Control > Queue Bandwidth Control Settings**, as show below:



Unit	From Port	To Port	From Queue	To Queue	Min Rate (64-1024000)	Max Rate (64-1024000)
1	01	01	0	0	☑ No Limit	☑ No Limit

Unit 1 Settings

Queue Bandwidth Control Table On Port 1

Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)
0	No Limit	No Limit
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit

Queue Bandwidth Control Table On Port 2

Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)
0	No Limit	No Limit
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit

Queue Bandwidth Control Table On Port 3

Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)
0	No Limit	No Limit
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit

Queue Bandwidth Control Table On Port 4

Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)

Figure 6-5 Queue Bandwidth Control Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
From Queue / To Queue	Use the drop-down menu to select the queue range to use for this configuration.
Min Rate (64-1024000)	Specify the packet limit, in Kbps that the ports are allowed to receive. Tick the **No limit** check box to have unlimited rate of packets received by the specified queue.

Max Rate (64-1024000)	Enter the maximum rate for the queue. For no limit select the **No Limit** option.

Click the **Apply** button to accept the changes made.

NOTE: The minimum granularity of queue bandwidth control is 64Kbit/sec. The system will adjust the number to the multiple of 64 automatically.

Traffic Control Settings

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase due to a malicious end station on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

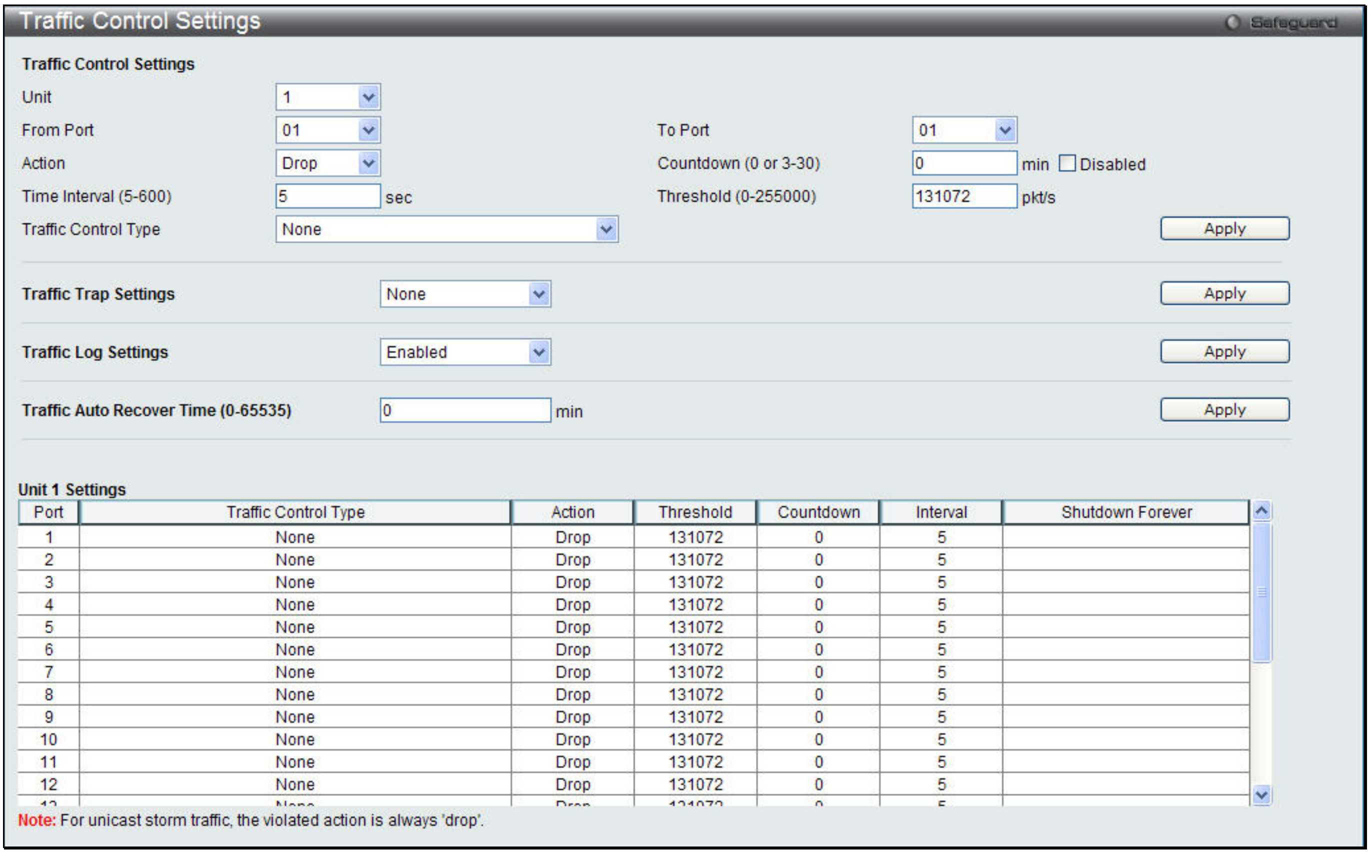
Packet storms are monitored to determine if too many packets are flooding the network based on threshold levels provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the *Drop* option of the Action parameter in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shut down the port to all incoming traffic, with the exception of STP BPDU packets, for a time period specified using the Count Down parameter.

If a Time Interval parameter times-out for a port configured for traffic control and a packet storm continues, that port will be placed in Shutdown Forever mode, which will cause a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the method of recovering the port is to manually recoup it using the **System Configuration > Port configuration > Port Settings** window or automatic recovering after the time period that is configured in the **Traffic Auto Recover Time** field. Select the disabled port and return its State to *Enabled* status. To utilize this method of Storm Control, choose the *Shutdown* option of the Action parameter in the window below.

Use this window to enable or disable storm control and adjust the threshold for multicast and broadcast storms.

To view the following window, click **QoS > Traffic Control Settings**, as show below:



Traffic Control Settings

Unit: 1

From Port: 01 | To Port: 01

Action: Drop | Countdown (0 or 3-30): 0 min ☐ Disabled

Time Interval (5-600): 5 sec | Threshold (0-255000): 131072 pkt/s

Traffic Control Type: None

Traffic Trap Settings: None

Traffic Log Settings: Enabled

Traffic Auto Recover Time (0-65535): 0 min

Unit 1 Settings

Port	Traffic Control Type	Action	Threshold	Countdown	Interval	Shutdown Forever
1	None	Drop	131072	0	5	
2	None	Drop	131072	0	5	
3	None	Drop	131072	0	5	
4	None	Drop	131072	0	5	
5	None	Drop	131072	0	5	
6	None	Drop	131072	0	5	
7	None	Drop	131072	0	5	
8	None	Drop	131072	0	5	
9	None	Drop	131072	0	5	
10	None	Drop	131072	0	5	
11	None	Drop	131072	0	5	
12	None	Drop	131072	0	5	

Note: For unicast storm traffic, the violated action is always 'drop'.

Figure 6-6 Traffic Control Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select the port range to use for this configuration.
Action	Select the method of traffic control from the drop-down menu. The choices are: *Drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. *Shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Count Down timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the port recovers after 5 minutes automatically or the user manually resets the port using the **Port Settings** window (**Configuration> Port Configuration> Port Settings**). Choosing this option obligates the user to configure the Time Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.
Countdown (0 or 3-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as *Shutdown* in their Action field and therefore will not operate for hardware-based Traffic Control implementations. The possible time settings for this field are *0* and *3* to *30* minutes. To disable this feature select the **Disable** option.
Time Interval (5-600)	The Time Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are

	the determining factor in deciding when incoming packets exceed the Threshold value. The Time Interval may be set between *5* and *600* seconds, with a default setting of *5* seconds.
Threshold (0-255000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from *0-255000* with a default setting of *131072* packets per second.
Traffic Control Type	Specifies the desired Storm Control Type: *None*, *Broadcast*, *Multicast*, *Unknown Unicast*, *Broadcast + Multicast*, *Broadcast + Unknown Unicast*, *Multicast + Unknown Unicast*, and *Broadcast + Multicast + Unknown Unicast*.
Traffic Trap Settings	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: *None* – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism. *Storm Occurred* – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. *Storm Cleared* – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. *Both* – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. This function cannot be implemented in the hardware mode. (When *Drop* is chosen for the Action parameter)
Traffic Log Settings	Use the drop-down menu to enable or disable the function. If enabled, the traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, the traffic control events are not logged.
Traffic Auto Recover Time (0-65535)	Enter the time allowed for auto recovery from shutdown for a port. The default value is 0, which means there is no auto recovery and the port remains in shutdown forever mode. This requires manual entry of the CLI command **config ports [<portlist> | all] state enable** to return the port to a forwarding state.

Click the **Apply** button to accept the changes made for each individual section.

NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).

NOTE: Ports that are in the Shutdown Forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch’s CPU.

NOTE: Ports that are in Shutdown Forever mode will be seen as link down in all windows and screens until the user recovers these ports.

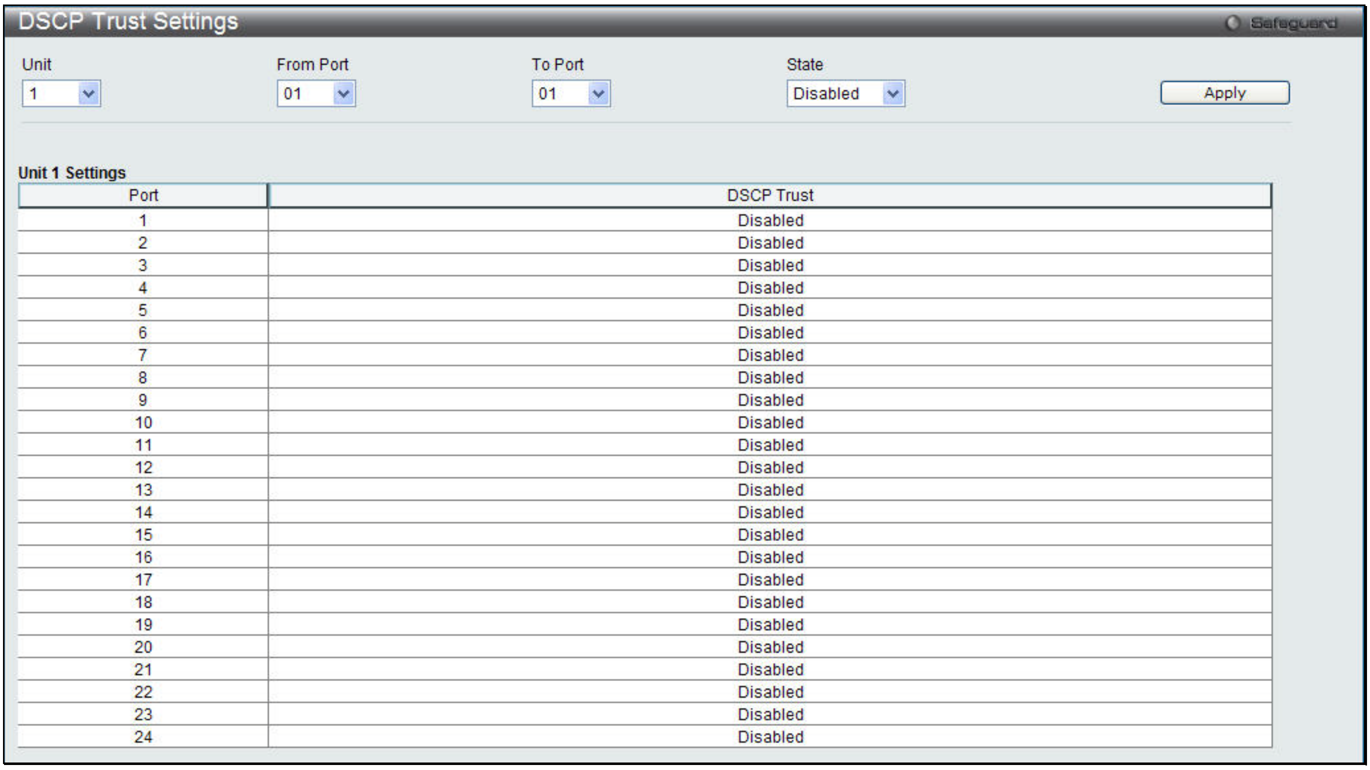
NOTE: The minimum granularity of storm control on a GE port is 1pps.

DSCP

DSCP Trust Settings

This page is to configure the DSCP trust state of ports. When ports are under the DSCP trust mode, the switch will insert the priority tag to untagged packets by using the DSCP Map settings instead of the default port priority.

To view the following window, click **QoS > DSCP > DSCP Trust Settings**, as show below:



Unit: 1
From Port: 01
To Port: 01
State: Disabled

Unit 1 Settings

Port	DSCP Trust
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

Figure 6-7 DSCP Trust Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select a range of port to configure.
State	Enable/disable to trust DSCP. By default, DSCP trust is disabled.

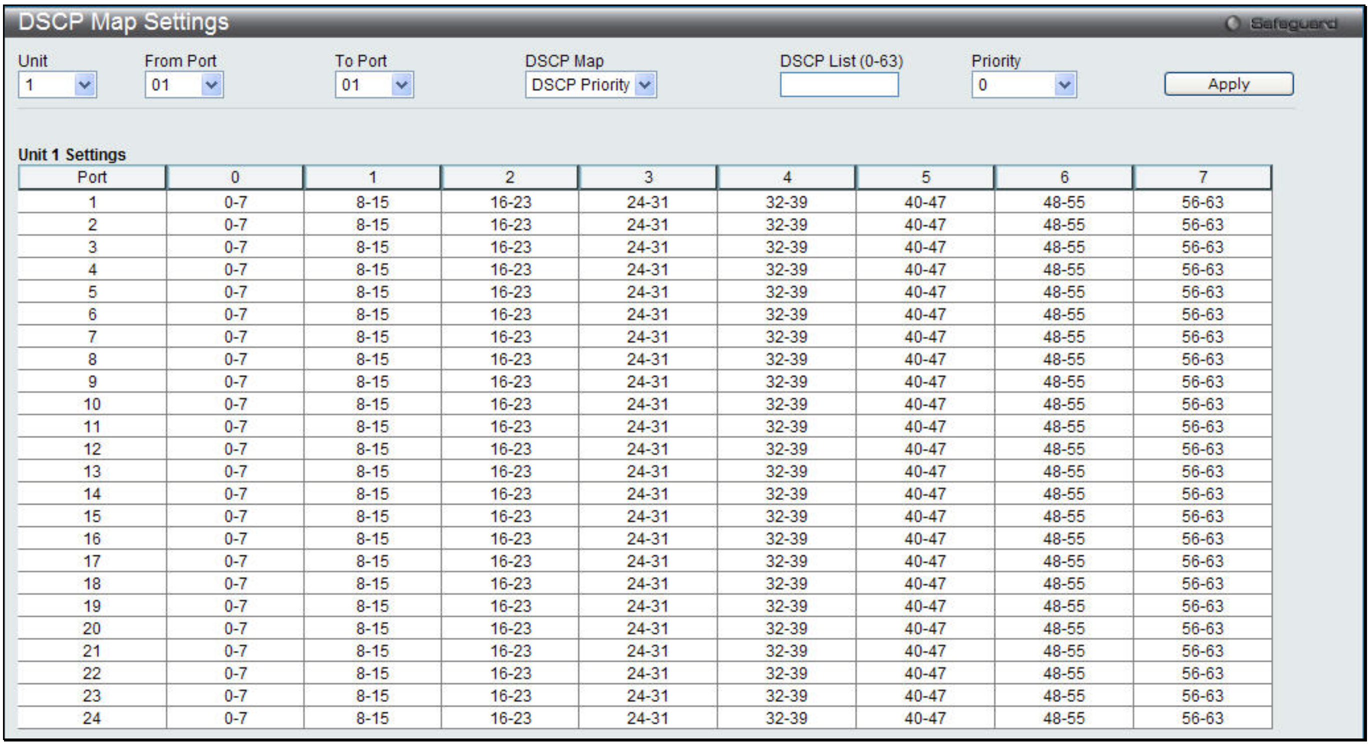
Click the **Apply** button to accept the changes made.

DSCP Map Settings

The mapping of DSCP to queue will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state.

The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingresses to the port. The remaining processing of the packet will base on the new DSCP. By default, the DSCP is mapped to the same DSCP.

To view the following window, click **QoS > DSCP > DSCP Map Settings**, as show below:



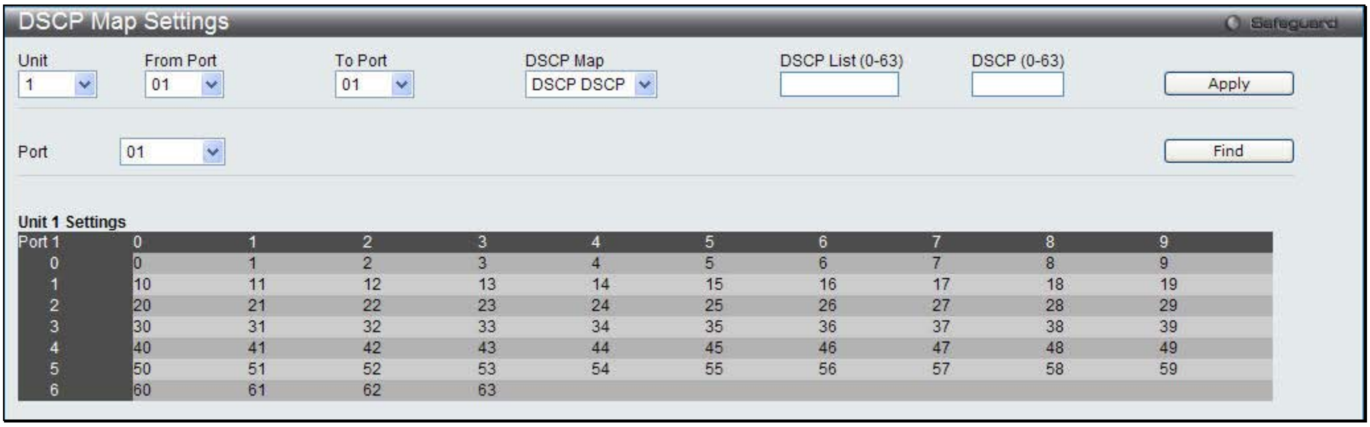
Unit: 1
From Port: 01
To Port: 01
DSCP Map: DSCP Priority
DSCP List (0-63):
Priority: 0

Unit 1 Settings

Port	0	1	2	3	4	5	6	7
1	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
2	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
3	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
4	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
5	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
6	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
7	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
8	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
9	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
10	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
11	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
12	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
13	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
14	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
15	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
16	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
17	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
18	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
19	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
20	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
21	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
22	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
23	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
24	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Figure 6-8 DSCP Map Settings - DSCP Priority window

To view the following window, click **QoS > DSCP > DSCP Map Settings** and select **DSCP DSCP** from the DSCP Map drop-down menu, as show below:



Unit: 1
From Port: 01
To Port: 01
DSCP Map: DSCP DSCP
DSCP List (0-63):
DSCP (0-63):
Port: 01

Unit 1 Settings

Port 1	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	10	11	12	13	14	15	16	17	18	19
2	20	21	22	23	24	25	26	27	28	29
3	30	31	32	33	34	35	36	37	38	39
4	40	41	42	43	44	45	46	47	48	49
5	50	51	52	53	54	55	56	57	58	59
6	60	61	62	63						

Figure 6-9 DSCP Map Settings - DSCP DSCP window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menu to select a range of port to configure.
DSCP Map	Use the drop-down menu to select one of two options: *DSCP Priority* – Specifies a list of DSCP values to be mapped to a specific priority. *DSCP DSCP* – Specifies a list of DSCP value to be mapped to a specific DSCP.
DSCP List (0-63)	Enter a DSCP List value.
Priority	Use the drop-down menu to select a Priority value. This appears when selecting **DSCP Priority** in the **DSCP Map** drop-down menu.
DSCP (0-63)	Enter a DSCP value. This appears when selecting **DSCP Priority** in the **DSCP DSCP** drop-down menu.
Port	Use the drop-down menu to select a port

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

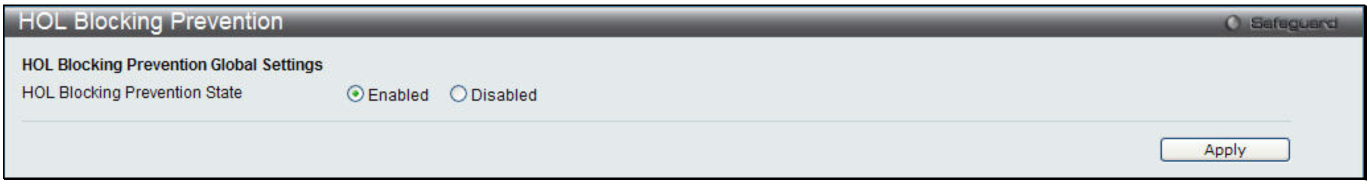
HOL Blocking Prevention

HOL (Head of Line) Blocking happens when one of the destination ports of a broadcast or multicast packet are busy. The switch will hold this packet in the buffer while the other destination port will not transmit the packet even they are not busy.

The HOL Blocking Prevention will ignore the busy port and forward the packet directly to have lower latency and better performance.

On this page the user can enable or disable HOL Blocking Prevention.

To view the following window, click **QoS > HOL Blocking Prevention**, as show below:



HOL Blocking Prevention Global Settings

HOL Blocking Prevention State ● Enabled ○ Disabled

Figure 6-10 HOL blocking Prevention window

The fields that can be configured are described below:

Parameter	Description
HOL Blocking Prevention State	Click the radio buttons to enable of disable the HOL blocking prevention global settings.

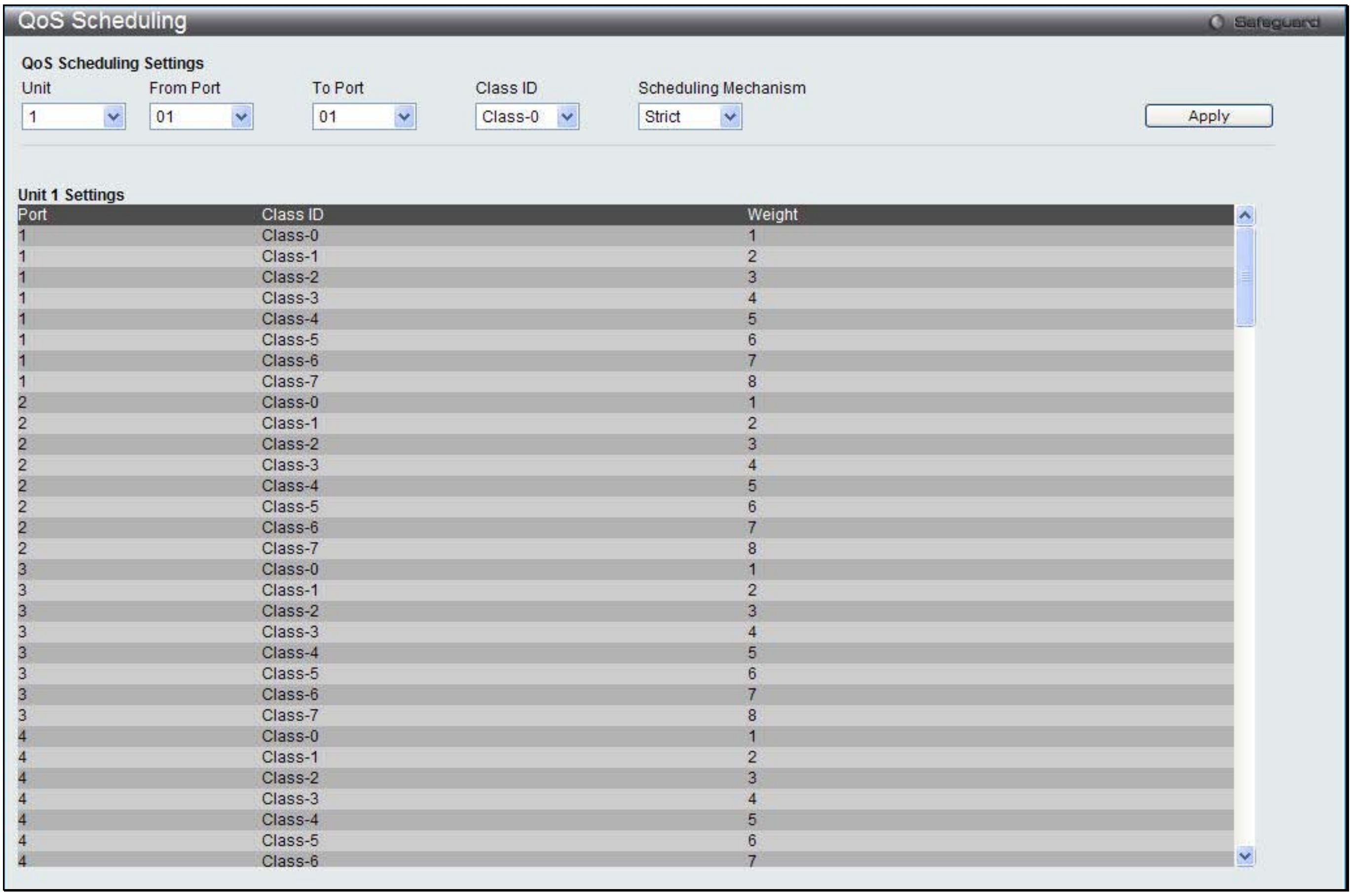
Click the **Apply** button to accept the changes made.

Scheduling Settings

QoS Scheduling

This window allows the user to configure the way the Switch will map an incoming packet per port based on its 802.1p user priority, to one of the eight available hardware priority queues available on the Switch.

To view this window, click **QoS > Scheduling Settings > QoS Scheduling** as shown below:



QoS Scheduling Settings

Unit: 1
From Port: 01
To Port: 01
Class ID: Class-0
Scheduling Mechanism: Strict

Unit 1 Settings

Port	Class ID	Weight
1	Class-0	1
1	Class-1	2
1	Class-2	3
1	Class-3	4
1	Class-4	5
1	Class-5	6
1	Class-6	7
1	Class-7	8
2	Class-0	1
2	Class-1	2
2	Class-2	3
2	Class-3	4
2	Class-4	5
2	Class-5	6
2	Class-6	7
2	Class-7	8
3	Class-0	1
3	Class-1	2
3	Class-2	3
3	Class-3	4
3	Class-4	5
3	Class-5	6
3	Class-6	7
3	Class-7	8
4	Class-0	1
4	Class-1	2
4	Class-2	3
4	Class-3	4
4	Class-4	5
4	Class-5	6
4	Class-6	7

Figure 6-11 QoS Scheduling window

The following parameters can be configured:

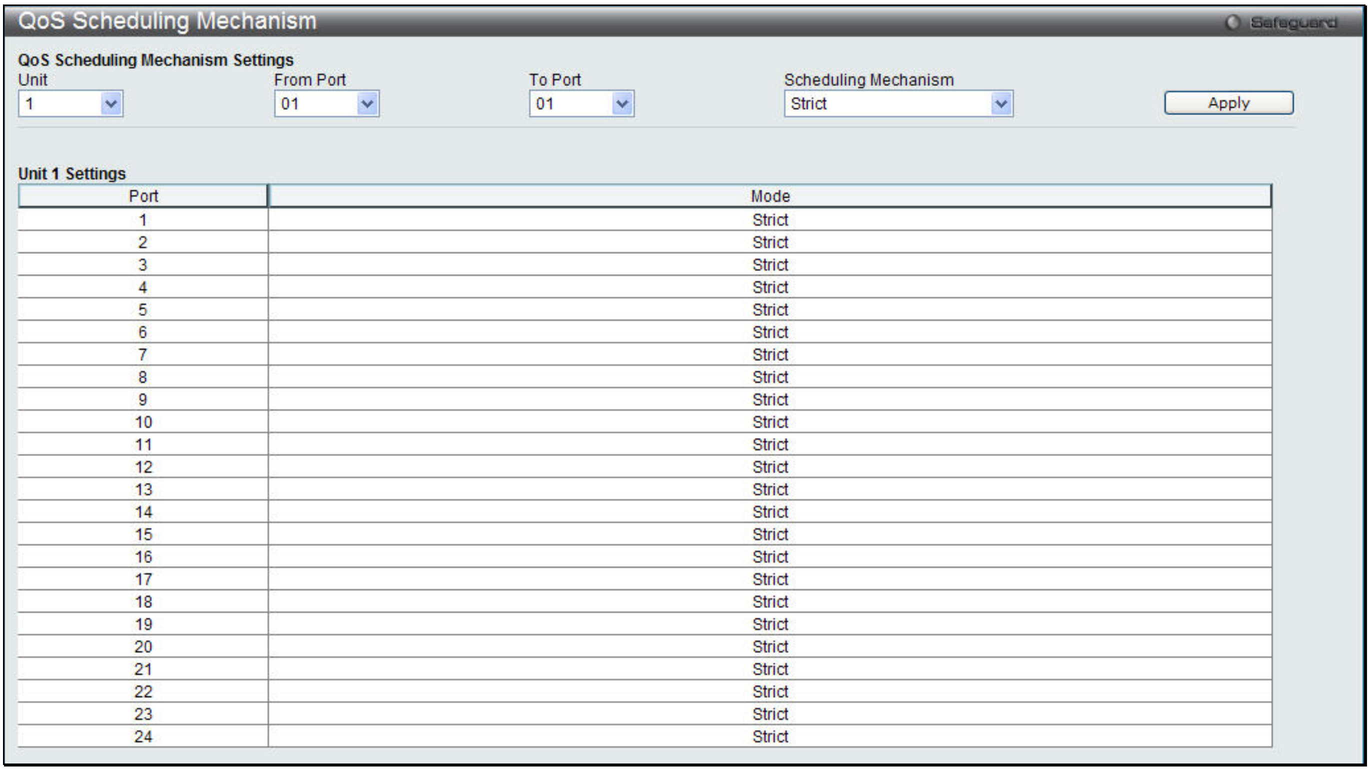
Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Enter the port or port list you wish to configure.
Class ID	Select the Class ID, from *0-7* to configure for the QoS parameters.
Scheduling Mechanism	*Strict* – The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weight* – Use the weighted round-robin (*WRR*) algorithm to handle packets in an even distribution in priority classes of service.

Click the **Apply** button to accept the changes made.

QoS Scheduling Mechanism

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delays. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > Scheduling Settings > QoS Scheduling Mechanism** as shown below:



QoS Scheduling Mechanism Settings

Unit: 1
From Port: 01
To Port: 01
Scheduling Mechanism: Strict

Unit 1 Settings

Port	Mode
1	Strict
2	Strict
3	Strict
4	Strict
5	Strict
6	Strict
7	Strict
8	Strict
9	Strict
10	Strict
11	Strict
12	Strict
13	Strict
14	Strict
15	Strict
16	Strict
17	Strict
18	Strict
19	Strict
20	Strict
21	Strict
22	Strict
23	Strict
24	Strict

Figure 6-12 QoS Scheduling Mechanism

The following parameters can be configured:

Parameter	Description
Unit	Select the unit you wish to configure.
From Port / To Port	Enter the port or port list you wish to configure.
Scheduling Mechanism	*Strict* – The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty. *Weighted Round Robin* – Use the weighted round-robin algorithm to handle packets in an even distribution in priority classes of service.

Click the **Apply** button to accept the changes made.

NOTE: The settings you assign to the queues, numbers 0-7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

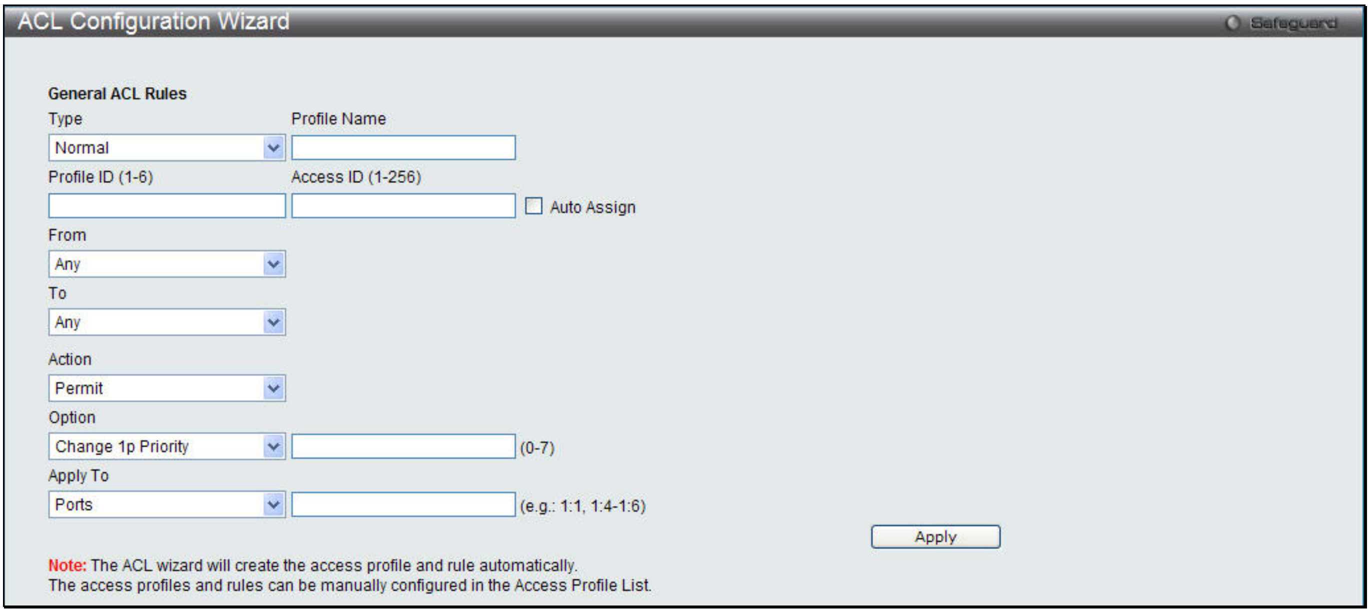
Chapter 7 ACL

ACL Configuration Wizard
Access Profile List
CPU Access Profile List
ACL Finder
ACL Flow Meter
Egress Access Profile List (EI Mode Only)
Egress ACL Flow Meter (EI Mode Only)

ACL Configuration Wizard

The ACL Configuration Wizard will aid the user in the creation of access profiles and ACL Rules automatically by simply inputting the address or service type and the action needed. It saves administrators a lot of time.

To view this window, click **ACL > ACL Configuration Wizard** as shown below:



Type: Normal
From: Any
To: Any
Action: Permit
Option: Change 1p Priority
Apply To: Ports

Note: The ACL wizard will create the access profile and rule automatically.
The access profiles and rules can be manually configured in the Access Profile List.

Figure 7-1 ACL Configuration Wizard window

The fields that can be configured are described below:

Parameter	Description
Type	Use the drop-down menu to select the general ACL Rule types: *Normal* – Selecting this option will create a Normal ACL Rule. *CPU* – Selecting this option will create a CPU ACL Rule. *Egress* **(EI Mode Only)** - Selecting this option will create an Egress ACL Rule.
Profile Name	After selecting to configure a **Normal** type rule, the user can enter the Profile Name for the new rule here.
Profile ID (1-6)	Enter the Profile ID for the new rule.
Access ID (1-256)	Enter the Access ID for the new rule. Selecting the **Auto Assign** option will allow the switch to automatically assign an unused access ID to this rule.
From / To	This rule can be created to apply to four different categories: *Any* – Selecting this option will include any starting category to this rule. *MAC Address* – Selecting this option will allow the user to enter a range of MAC addresses for this rule. *IPv4 Address* – Selecting this option will allow the user to enter a range of IPv4

	addresses for this rule. *IPv6* – Selecting this option will allow the user to enter a range of IPv6 addresses for this rule.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the mirror port section. Port Mirroring must be enabled and a target port must be set.
Option	After selecting the **Permit** action, the user can select one of the following options: *Change 1p Priority* – Here the user can enter the 1p priority value. *Replace DSCP* – Here the user can enter the DSCP value. *Replace ToS Precedence* – Here the user can enter the ToS Precedence value.
Apply To	Use the drop-down menu to select and enter the information that this rule will be applied to. *Ports* – Enter a port number or a port range. *VLAN Name* – Enter a VLAN name. *VLAN ID* – Enter a VLAN ID.

Click the **Apply** button to accept the changes made.

NOTE: The Switch will use one minimum mask to cover all the terms that user input, however, some extra bits may also be masked at the same time. To optimize the ACL profile and rules, please use manual configuration.

Access Profile List

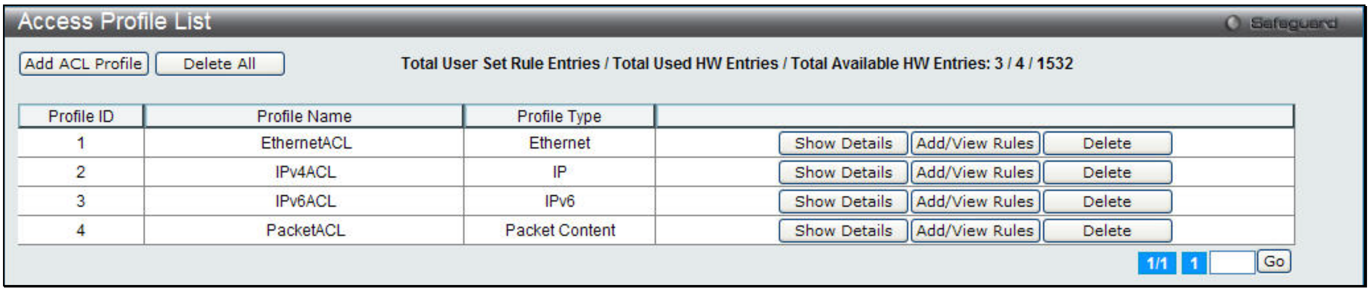
Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header.

To view Access Profile List window, click **ACL > Access Profile List** as shown below:

The Switch supports four Profile Types, Ethernet ACL, IPv4 ACL, IPv6 ACL, and Packet Content ACL.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

Users can display the currently configured Access Profiles on the Switch.



Total User Set Rule Entries / Total Used HW Entries / Total Available HW Entries: 3 / 4 / 1532

Profile ID	Profile Name	Profile Type	
1	EthernetACL	Ethernet	Show Details Add/View Rules Delete
2	IPv4ACL	IP	Show Details Add/View Rules Delete
3	IPv6ACL	IPv6	Show Details Add/View Rules Delete
4	PacketACL	Packet Content	Show Details Add/View Rules Delete

Figure 7-2 Access Profile List window

Click the **Add ACL Profile** button to add an entry to the **Access Profile List**.

Click the **Delete All** button to remove all access profiles from this table.

Click the **Show Details** button to display the information of the specific profile ID entry.
Click the **Add/View Rules** button to view or add ACL rules within the specified profile ID.
Click the **Delete** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

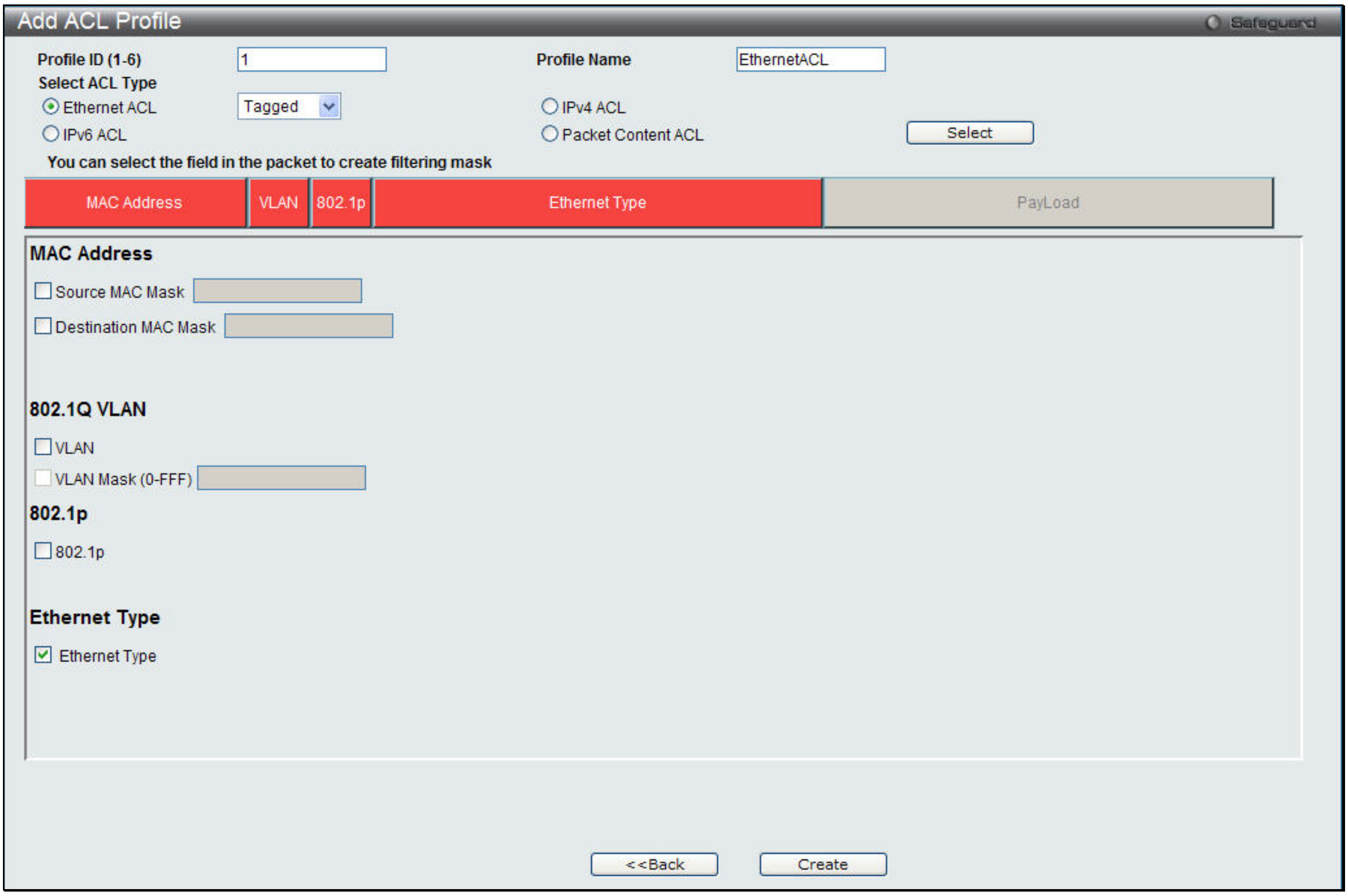
There are four **Add Access Profile** windows;

- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv6 address-based profile configuration,
- one for IPv4 address-based profile configuration, and
- one for packet content profile configuration.

Add an Ethernet ACL Profile

The window shown below is the Add ACL Profile window for Ethernet. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:



Add ACL Profile

Profile ID (1-6): 1
Profile Name: EthernetACL
Select ACL Type
● Ethernet ACL — Tagged
○ IPv4 ACL
○ IPv6 ACL
○ Packet Content ACL

You can select the field in the packet to create filtering mask

MAC Address
☐ Source MAC Mask
☐ Destination MAC Mask

802.1Q VLAN
☐ VLAN
☐ VLAN Mask (0-FFF)

802.1p
☐ 802.1p

Ethernet Type
☑ Ethernet Type

Figure 7-3 Add ACL Profile window (Ethernet ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Enter a unique identifier number for this profile set. This value can be set from *1* to *6.*
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile.

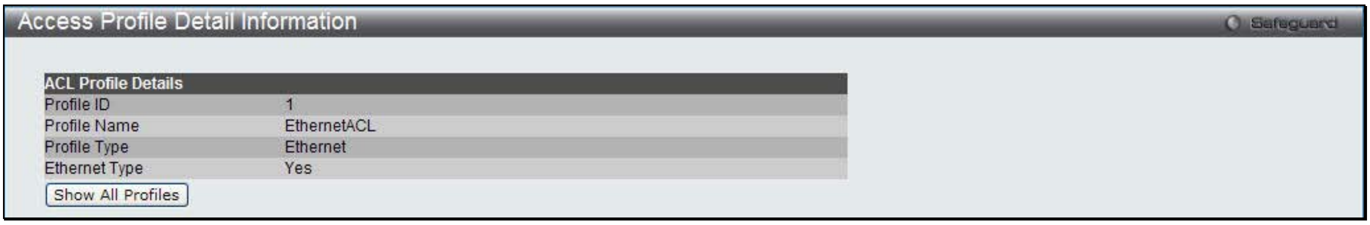
	Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame’s header.
Source MAC Mask	Enter a MAC address mask for the source MAC address, e.g. FF-FF-FF-FF-FF-FF.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address, e.g. FF-FF-FF-FF-FF-FF.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

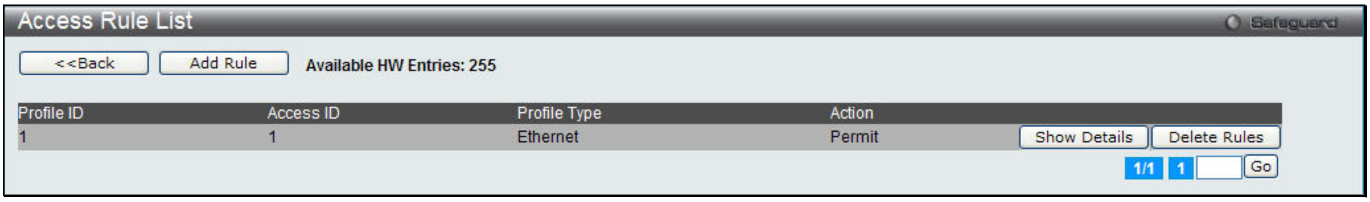


ACL Profile Details	
Profile ID	1
Profile Name	EthernetACL
Profile Type	Ethernet
Ethernet Type	Yes

Figure 7-4 Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



Available HW Entries: 255

Profile ID	Access ID	Profile Type	Action
1	1	Ethernet	Permit

Figure 7-5 Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.

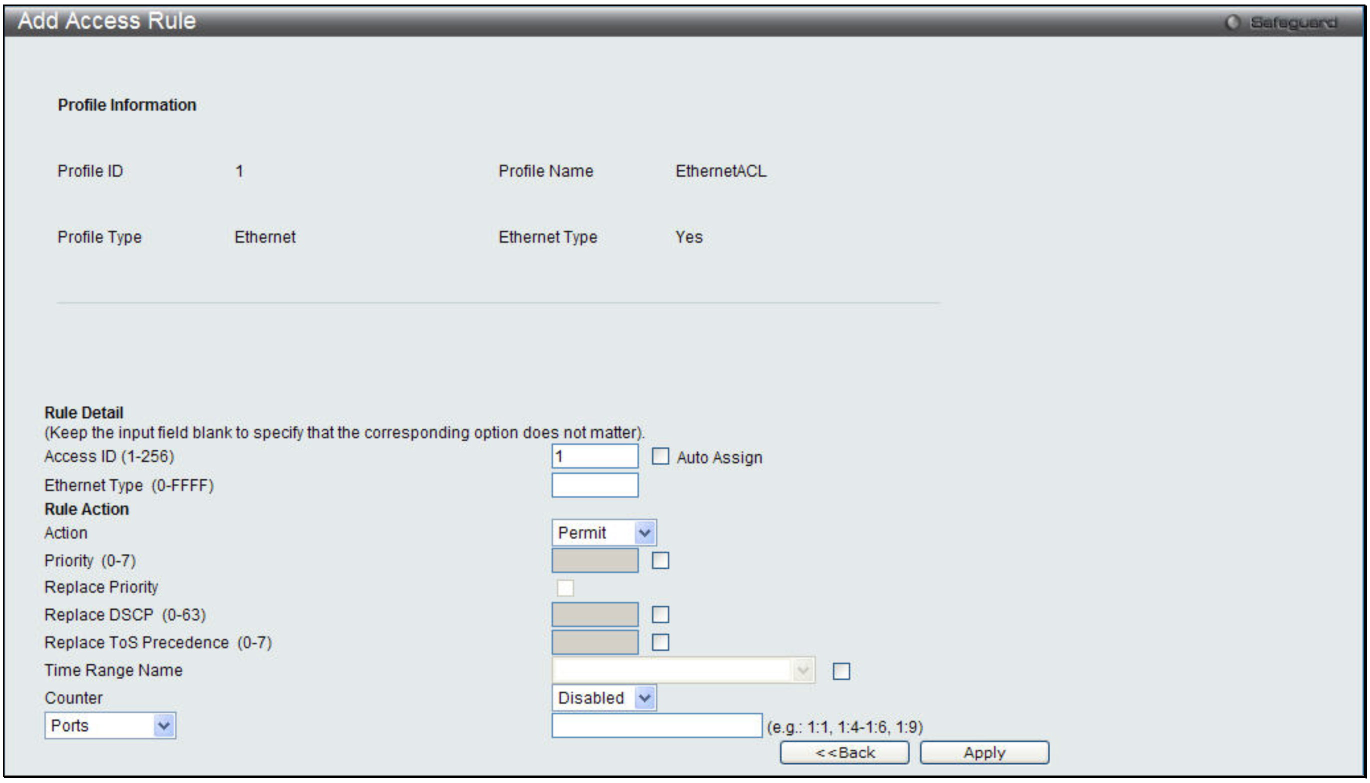
Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Add Access Rule

Profile Information

Profile ID 1

Profile Name EthernetACL

Profile Type Ethernet

Ethernet Type Yes

Rule Detail

(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256) 1 ☐ Auto Assign

Ethernet Type (0-FFFF)

Rule Action

Action Permit

Priority (0-7) ☐

Replace Priority ☐

Replace DSCP (0-63) ☐

Replace ToS Precedence (0-7) ☐

Time Range Name ☐

Counter Disabled

Ports (e.g.: 1:1, 1:4-1:6, 1:9)

Figure 7-6 Add Access Rule window (Ethernet ACL)

The fields that can be configured are described below:

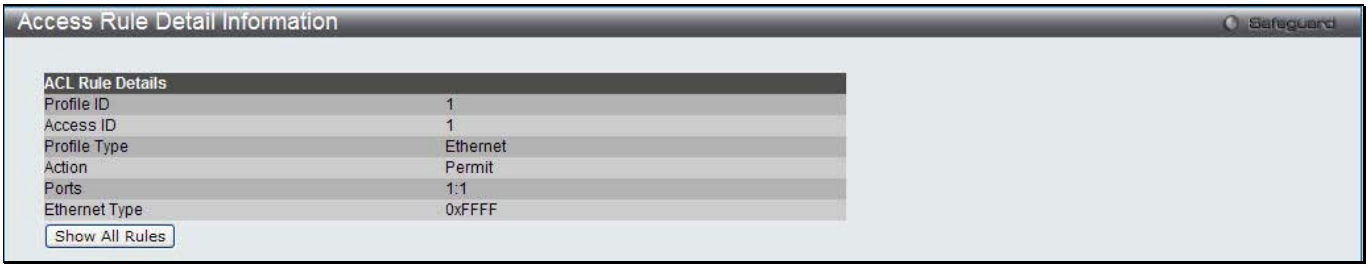
Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default traffic class.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times

	when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



ACL Rule Details	
Profile ID	1
Access ID	1
Profile Type	Ethernet
Action	Permit
Ports	1:1
Ethernet Type	0xFFFF

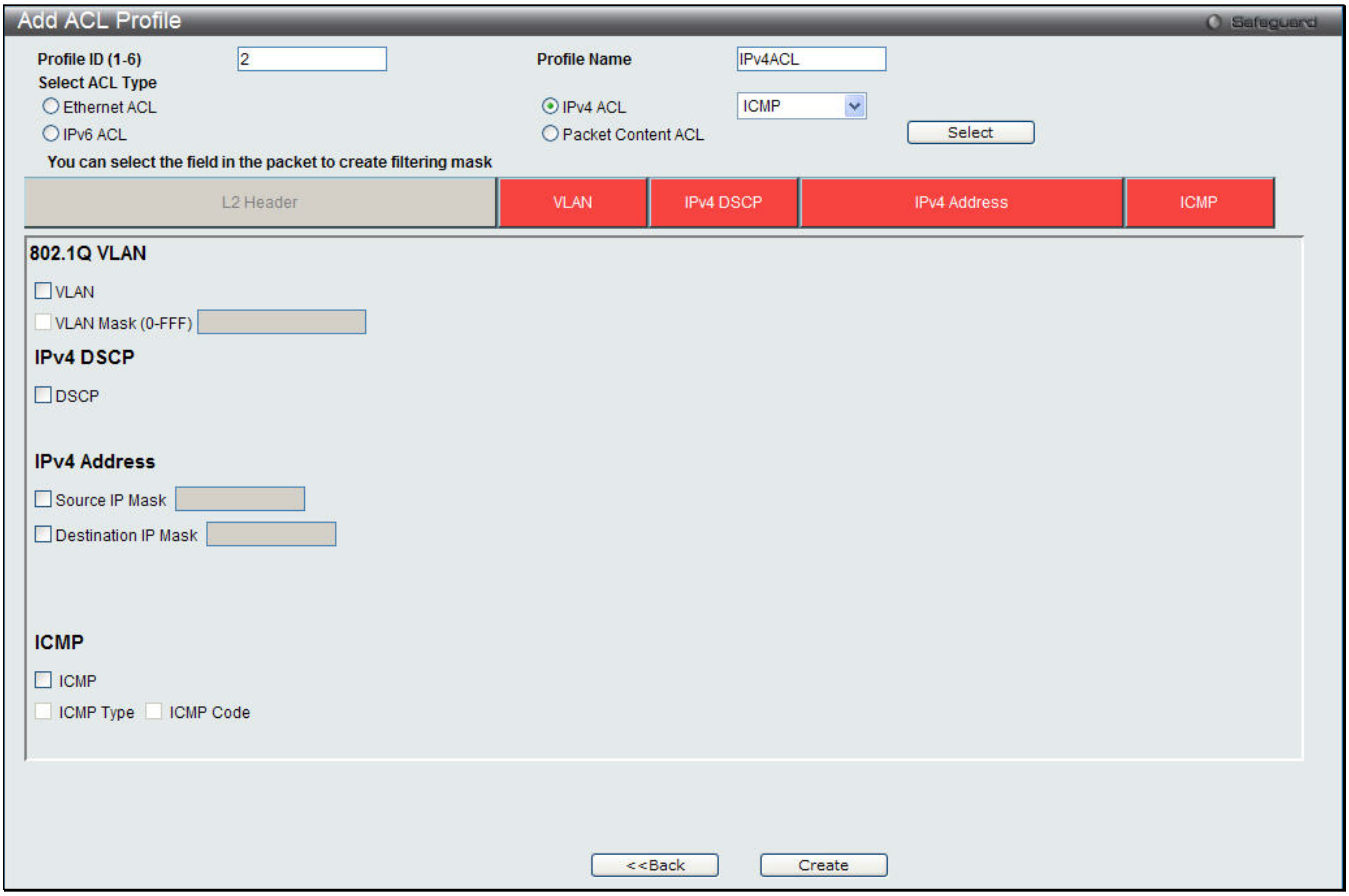
Figure 7-7 Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 ACL Profile

The window shown below is the Add ACL Profile window for IPv4. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:



Add ACL Profile

Profile ID (1-6) 2

Profile Name IPv4ACL

Select ACL Type

○ Ethernet ACL

● IPv4 ACL ICMP

○ IPv6 ACL

○ Packet Content ACL

You can select the field in the packet to create filtering mask

802.1Q VLAN

☐ VLAN

☐ VLAN Mask (0-FFF)

IPv4 DSCP

☐ DSCP

IPv4 Address

☐ Source IP Mask

☐ Destination IP Mask

ICMP

☐ ICMP

☐ ICMP Type ☐ ICMP Code

Figure 7-8 Add ACL Profile window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Enter a unique identifier number for this profile set. This value can be set from *1* to *6.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame’s header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address, e.g. 255.255.255.255.
IPv4 Destination IP Mask	Enter an IP address mask for the destination IP address, e.g. 255.255.255.255.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines:

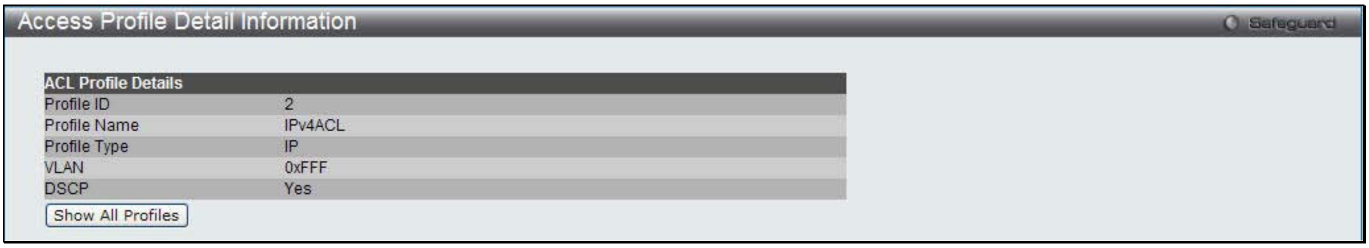
	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

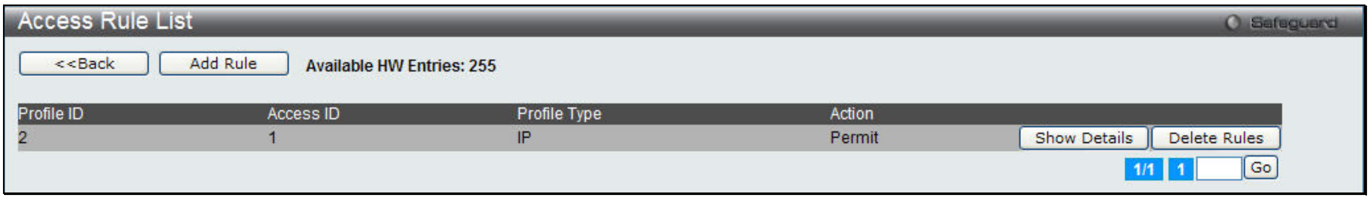


ACL Profile Details	
Profile ID	2
Profile Name	IPv4ACL
Profile Type	IP
VLAN	0xFFF
DSCP	Yes

Figure 7-9 Access Profile Detail Information window (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



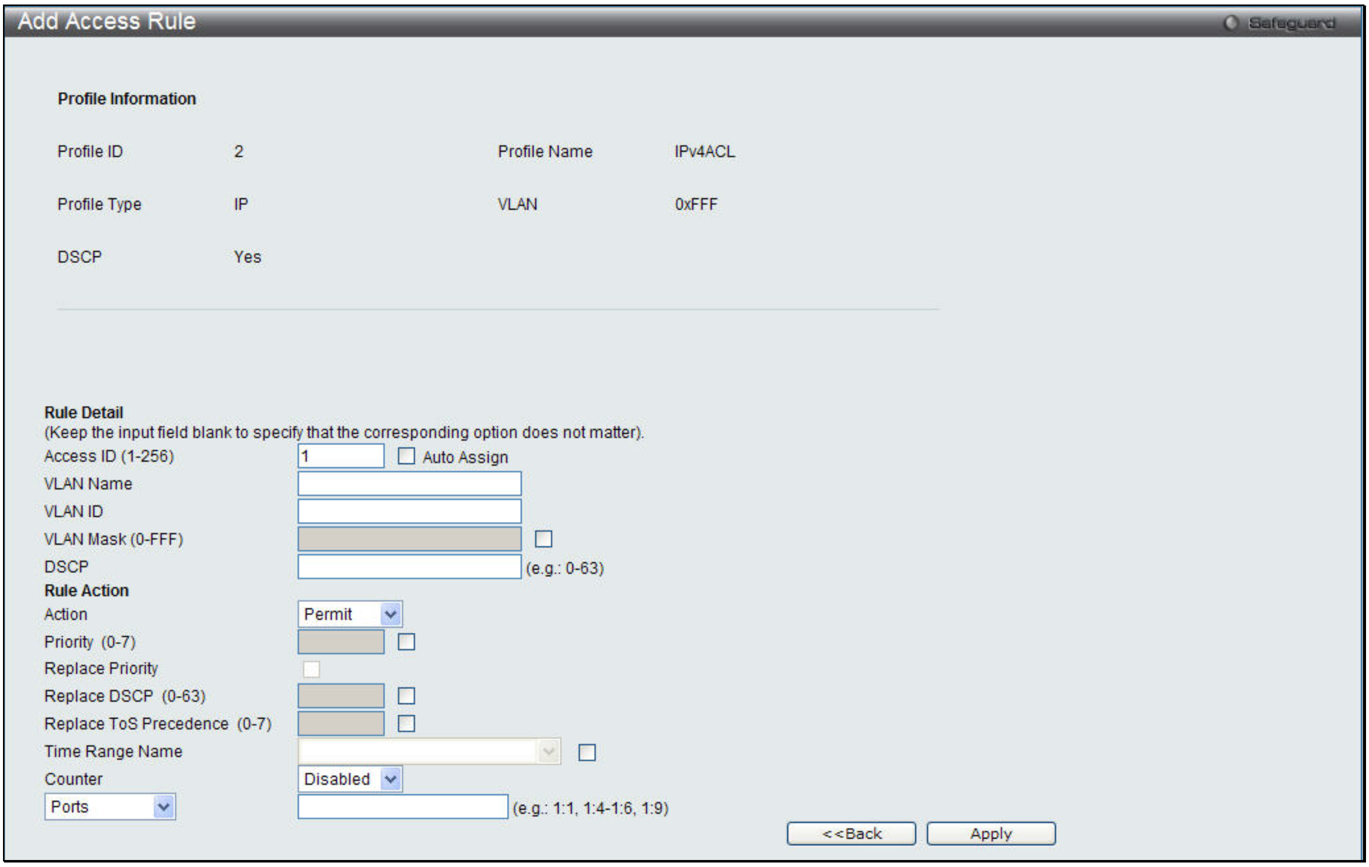
Available HW Entries: 255

Profile ID	Access ID	Profile Type	Action
2	1	IP	Permit

Figure 7-10 Access Rule List window (IPv4 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Profile Information

Profile ID: 2
Profile Name: IPv4ACL
Profile Type: IP
VLAN: 0xFFF
DSCP: Yes

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).
Access ID (1-256): 1
VLAN Name:
VLAN ID:
VLAN Mask (0-FFF):
DSCP:
Rule Action
Action: Permit
Priority (0-7):
Replace Priority:
Replace DSCP (0-63):
Replace ToS Precedence (0-7):
Time Range Name:
Counter: Disabled
Ports:

Figure 7-11 Add Access Rule (IPv4 ACL)

The fields that can be configured are described below:

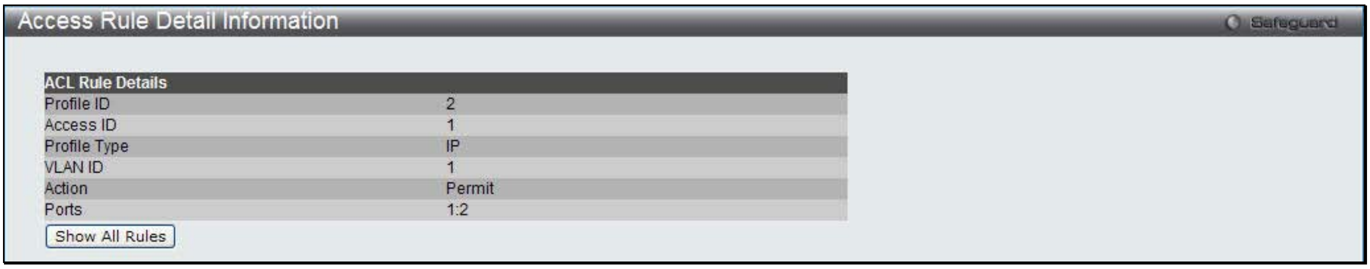
Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select Permit to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select Mirror to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.

Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



ACL Rule Details	
Profile ID	2
Access ID	1
Profile Type	IP
VLAN ID	1
Action	Permit
Ports	1:2

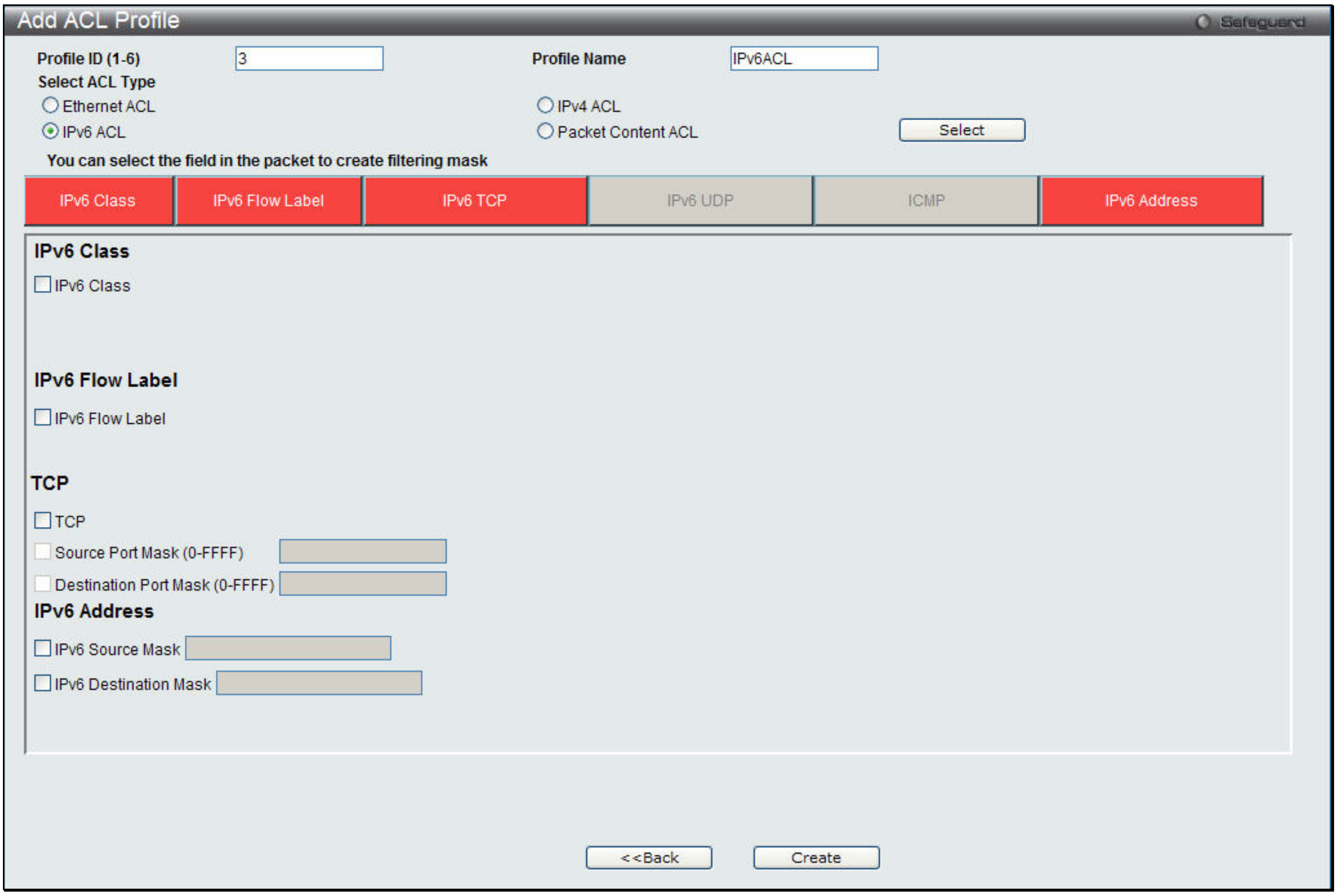
Figure 7-12 Access Rule Detail Information (IPv4 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile (EI Mode Only)

The window shown below is the Add ACL Profile window for IPv6. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:



Profile ID (1-6): 3
Profile Name: IPv6ACL
Select ACL Type
○ Ethernet ACL
● IPv6 ACL
○ IPv4 ACL
○ Packet Content ACL

You can select the field in the packet to create filtering mask

IPv6 Class
☐ IPv6 Class

IPv6 Flow Label
☐ IPv6 Flow Label

TCP
☐ TCP
☐ Source Port Mask (0-FFFF)
☐ Destination Port Mask (0-FFFF)

IPv6 Address
☐ IPv6 Source Mask
☐ IPv6 Destination Mask

Figure 7-13 Add ACL Profile window (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Enter a unique identifier number for this profile set. This value can be set from *1* to *6.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Ticking this check box will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports. *Destination Port Mask* – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the TCP source port range. *Destination Port Mask* – Specify the range of the TCP destination port mask.

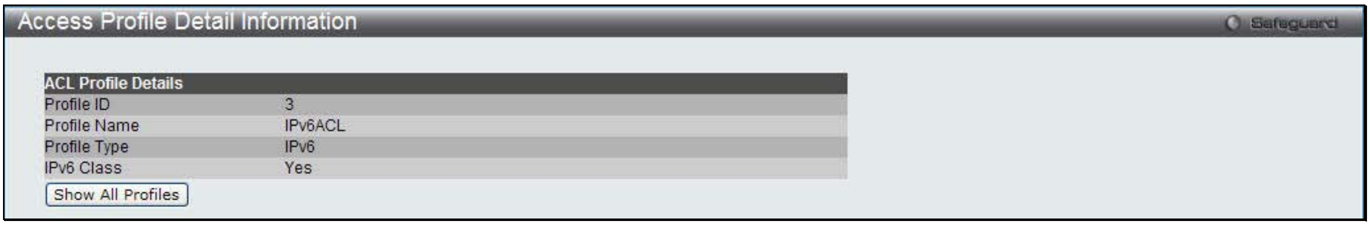
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
IPv6 Source Mask	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask.
IPv6 Destination Mask	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask.

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

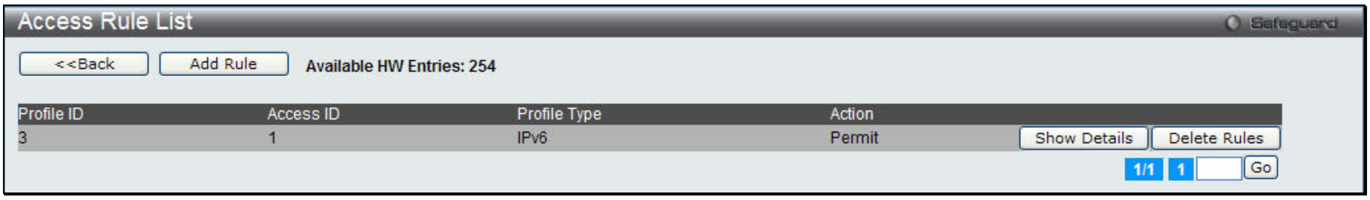


ACL Profile Details	
Profile ID	3
Profile Name	IPv6ACL
Profile Type	IPv6
IPv6 Class	Yes

Figure 7-14 Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



Available HW Entries: 254

Profile ID	Access ID	Profile Type	Action
3	1	IPv6	Permit

Figure 7-15 Access Rule List window (IPv6 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.

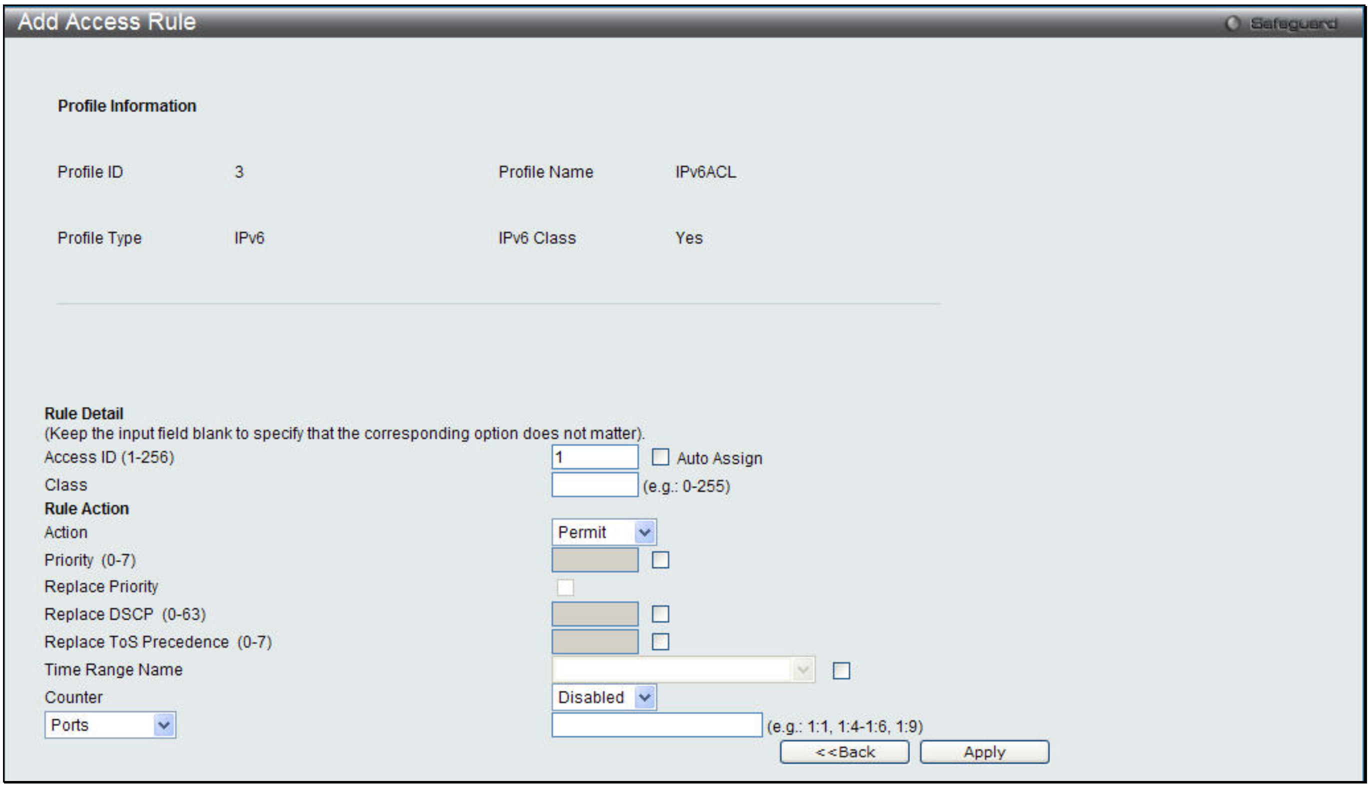
Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Add Access Rule

Profile Information

Profile ID	3	Profile Name	IPv6ACL
Profile Type	IPv6	IPv6 Class	Yes

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256)	1 ☐ Auto Assign
Class	(e.g.: 0-255)
Rule Action	
Action	Permit
Priority (0-7)	☐
Replace Priority	☐
Replace DSCP (0-63)	☐
Replace ToS Precedence (0-7)	☐
Time Range Name	☐
Counter	Disabled
Ports	(e.g.: 1:1, 1:4-1:6, 1:9)

Figure 7-16 Add Access Rule (IPv6 ACL)

The fields that can be configured are described below:

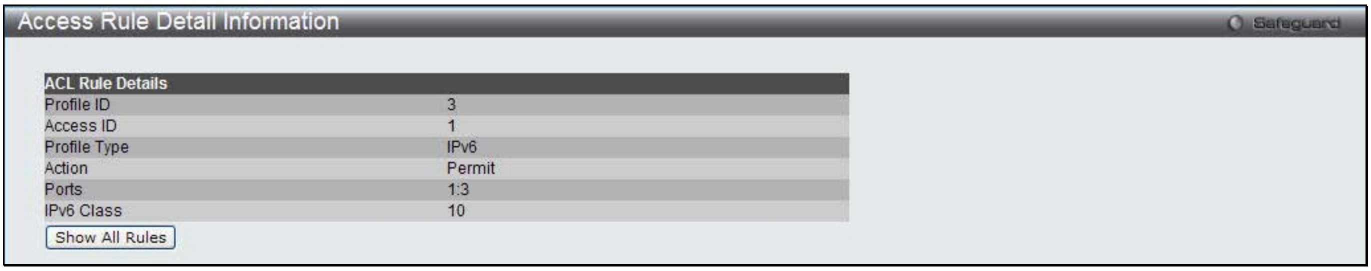
Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence (0-7)	Specify that the IP precedence of the outgoing packet is changed with the new value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been

	previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



ACL Rule Details	
Profile ID	3
Access ID	1
Profile Type	IPv6
Action	Permit
Ports	1:3
IPv6 Class	10

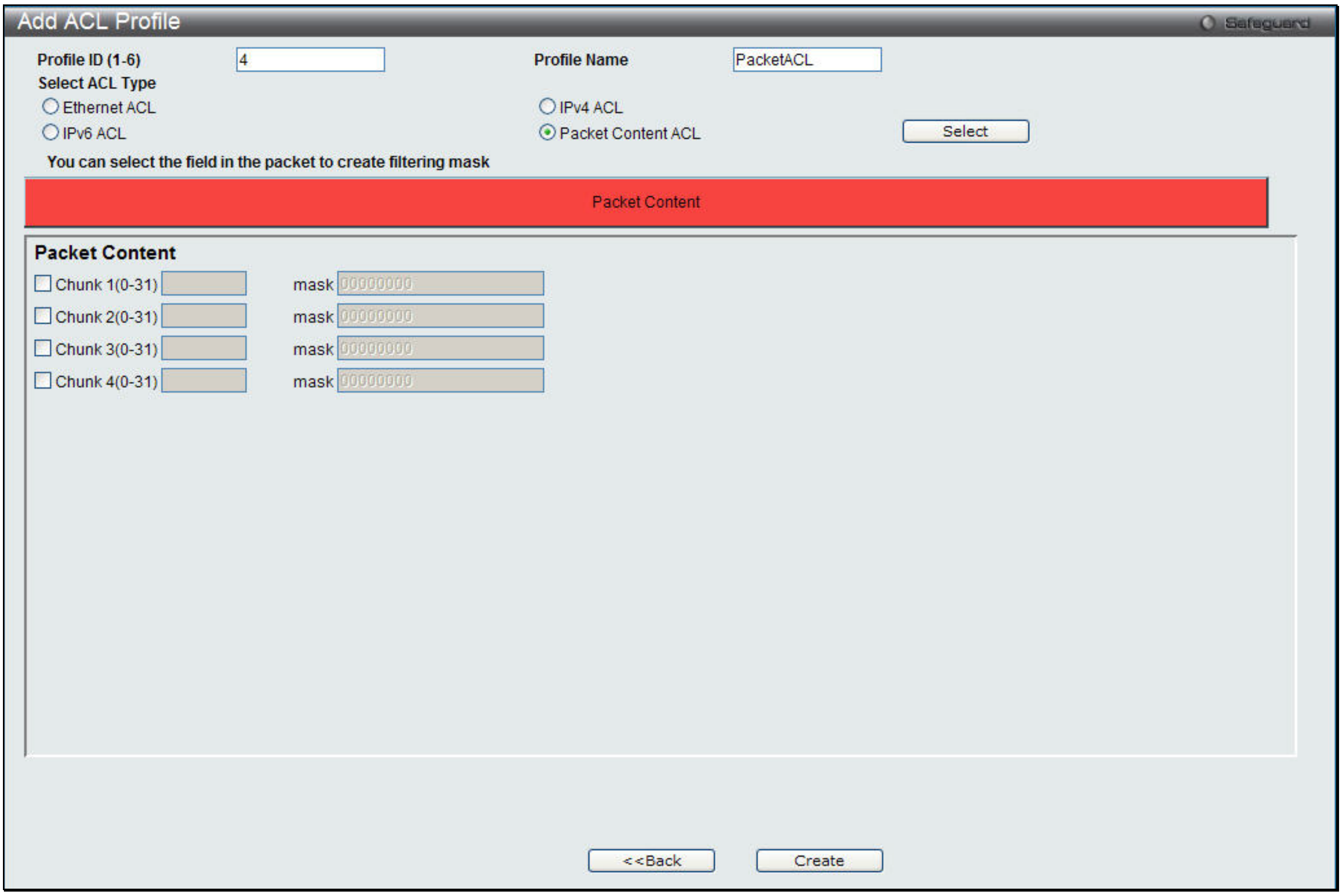
Figure 7-17 Access Rule Detail Information (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding a Packet Content ACL Profile

The window shown below is the Add ACL Profile window for Packet Content: To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add ACL Profile** button, the following page will appear:



Profile ID (1-6): 4

Profile Name: PacketACL

○ Ethernet ACL ○ IPv4 ACL ○ IPv6 ACL ● Packet Content ACL

Packet Content

☐ Chunk 1(0-31) mask 00000000
☐ Chunk 2(0-31) mask 00000000
☐ Chunk 3(0-31) mask 00000000
☐ Chunk 4(0-31) mask 00000000

.

Figure 7-18 Add ACL Profile (Packet Content ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-6)	Enter a unique identifier number for this profile set. This value can be set from *1* to *6.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header. Select Packet Content to instruct the Switch to examine the packet content in each frame's header.
Packet Content	Allows users to examine up to 4 specified offset_chunks within a packet at one time and specifies the frame content offset and mask. There are 4 chunk offsets and masks that can be configured. A chunk mask presents 4 bytes. 4 offset_chunks can be selected from a possible 32 predefined offset_chunks as described below: offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4.

chunk0	chunk1	chunk2	……	chunk29	chunk30	chunk31
B126, B127,	B2, B3,	B6, B7,	……	B114, B115,	B118, B119,	B122, B123,

B0, B1	B4, B5	B8, B9		B116, B117	B120, B121	B124, B125

Example:
offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1

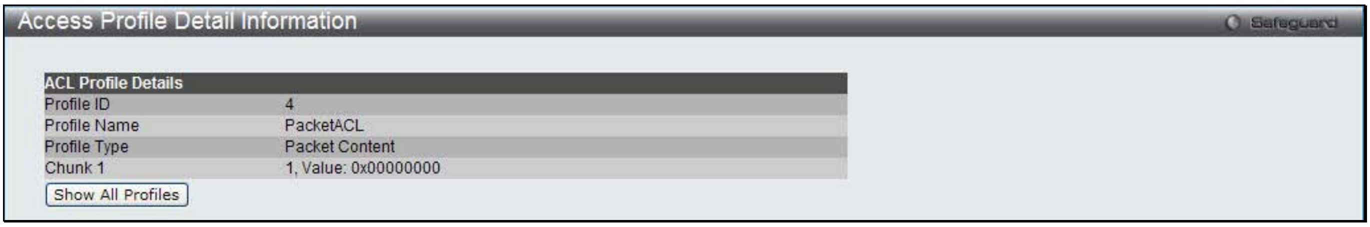
offset_chunk_1 0 0x0000ffff will match packet byte offset,0,1

NOTE: Only one packet_content_mask profile can be created.

With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), the D-Link xStack® switch family can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is why the Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

Click the **Select** button to select an ACL type.
Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:



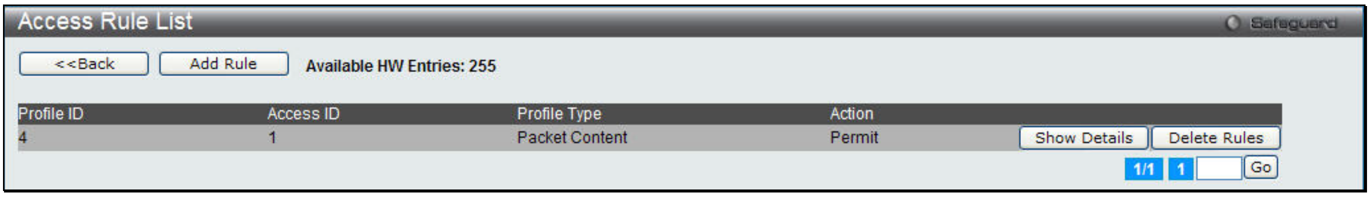
ACL Profile Details	
Profile ID	4
Profile Name	PacketACL
Profile Type	Packet Content
Chunk 1	1, Value: 0x00000000

Figure 7-19 Access Profile Detail Information (Packet Content ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (i.e. an ARP spoofing attack). For a more detailed explanation on how ARP protocol works and how to employ D-Link's unique Packet Content ACL to prevent ARP spoofing attack, please see Appendix E at the end of this manual.

After clicking the **Add/View Rules** button, the following page will appear:



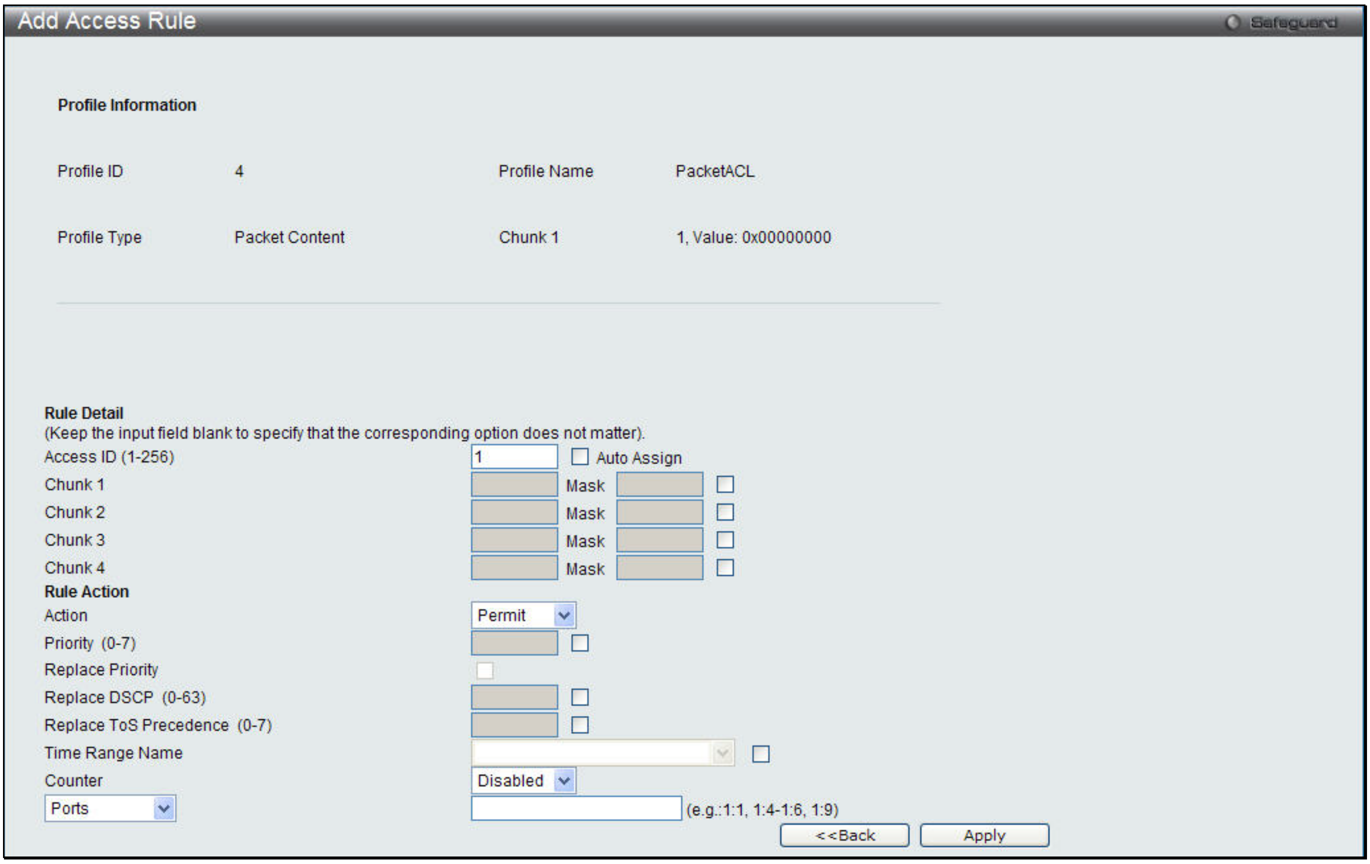
Available HW Entries: 255

Profile ID	Access ID	Profile Type	Action
4	1	Packet Content	Permit

Figure 7-20 Access Rule List (Packet Content ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Profile Information

Profile ID	4	Profile Name	PacketACL
Profile Type	Packet Content	Chunk 1	1, Value: 0x00000000

Rule Detail

(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256) 1 ☐ Auto Assign

Chunk 1 Mask ☐

Chunk 2 Mask ☐

Chunk 3 Mask ☐

Chunk 4 Mask ☐

Rule Action

Action Permit

Priority (0-7) ☐

Replace Priority ☐

Replace DSCP (0-63) ☐

Replace ToS Precedence (0-7) ☐

Time Range Name ☐

Counter Disabled

Ports (e.g.:1:1, 1:4-1:6, 1:9)

Figure 7-21 Add Access Rule (Packet Content ACL)

The fields that can be configured are described below:

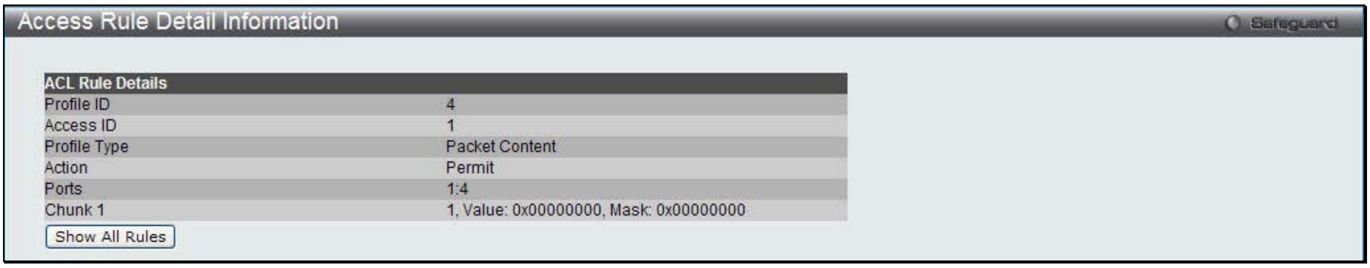
Parameter	Description
Access ID (1-256)	Type in a unique identifier number for this access. This value can be set from *1* to *256.* Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered. Select *Mirror* to specify that packets that match the access profile are mirrored to a port defined in the config mirror port command. Port Mirroring must be enabled and a target port must be set.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace Priority	Tick this check box to replace the Priority value in the adjacent field.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Replace ToS Precedence	Specify that the IP precedence of the outgoing packet is changed with the new

(0-7)	value. If used without an action priority, the packet is sent to the default TC.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



ACL Rule Details	
Profile ID	4
Access ID	1
Profile Type	Packet Content
Action	Permit
Ports	1:4
Chunk 1	1, Value: 0x00000000, Mask: 0x00000000

Figure 7-22 Access Rule Detail Information (Packet Content ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

CPU Access Profile List

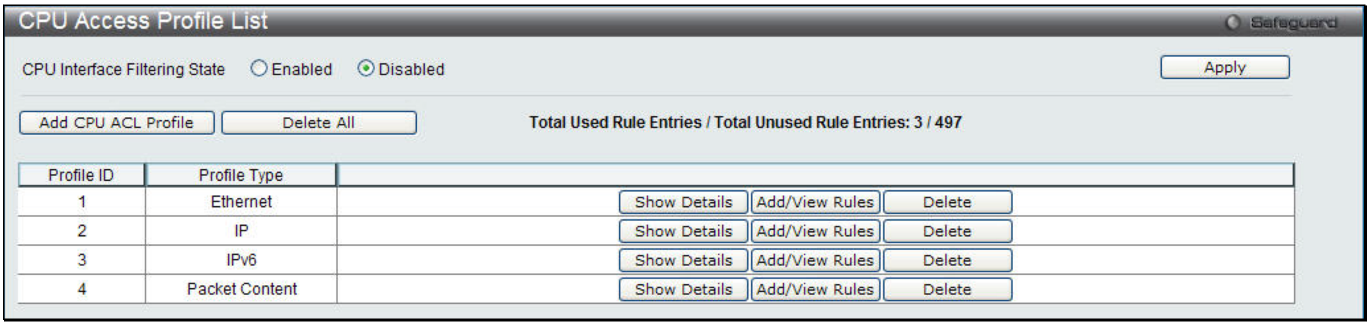
Due to a chipset limitation and needed extra switch security, the Switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the Switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

NOTE: CPU Interface Filtering is used to control traffic access to the switch directly such as protocols transition or management access. A CPU interface filtering rule won't impact normal L2/3 traffic forwarding. However, an improper CPU interface filtering rule may cause the network to become unstable.

To view CPU Access Profile List window, click **ACL > CPU Access Profile List** as shown below:

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.

Users may globally enable or disable the CPU Interface Filtering State mechanism by using the radio buttons to change the running state. Choose Enabled to enable CPU packets to be scrutinized by the Switch and Disabled to disallow this scrutiny.



CPU Interface Filtering State ○ Enabled ● Disabled

Total Used Rule Entries / Total Unused Rule Entries: 3 / 497

Profile ID	Profile Type	
1	Ethernet	Show Details Add/View Rules Delete
2	IP	Show Details Add/View Rules Delete
3	IPv6	Show Details Add/View Rules Delete
4	Packet Content	Show Details Add/View Rules Delete

Figure 7-23 CPU Access Profile List window

The fields that can be configured are described below:

Parameter	Description
CPU Interface Filtering State	Click to enable or disable the CPU interface filtering state.

Click the **Apply** button to accept the changes made.

Click the **Add CPU ACL Profile** button to add an entry to the **CPU ACL Profile List**.
Click the **Delete All** button to remove all access profiles from this table.
Click the **Show Details** button to display the information of the specific profile ID entry.
Click the **Add/View Rules** button to view or add CPU ACL rules within the specified profile ID.
Click the **Delete** button to remove the specific entry.

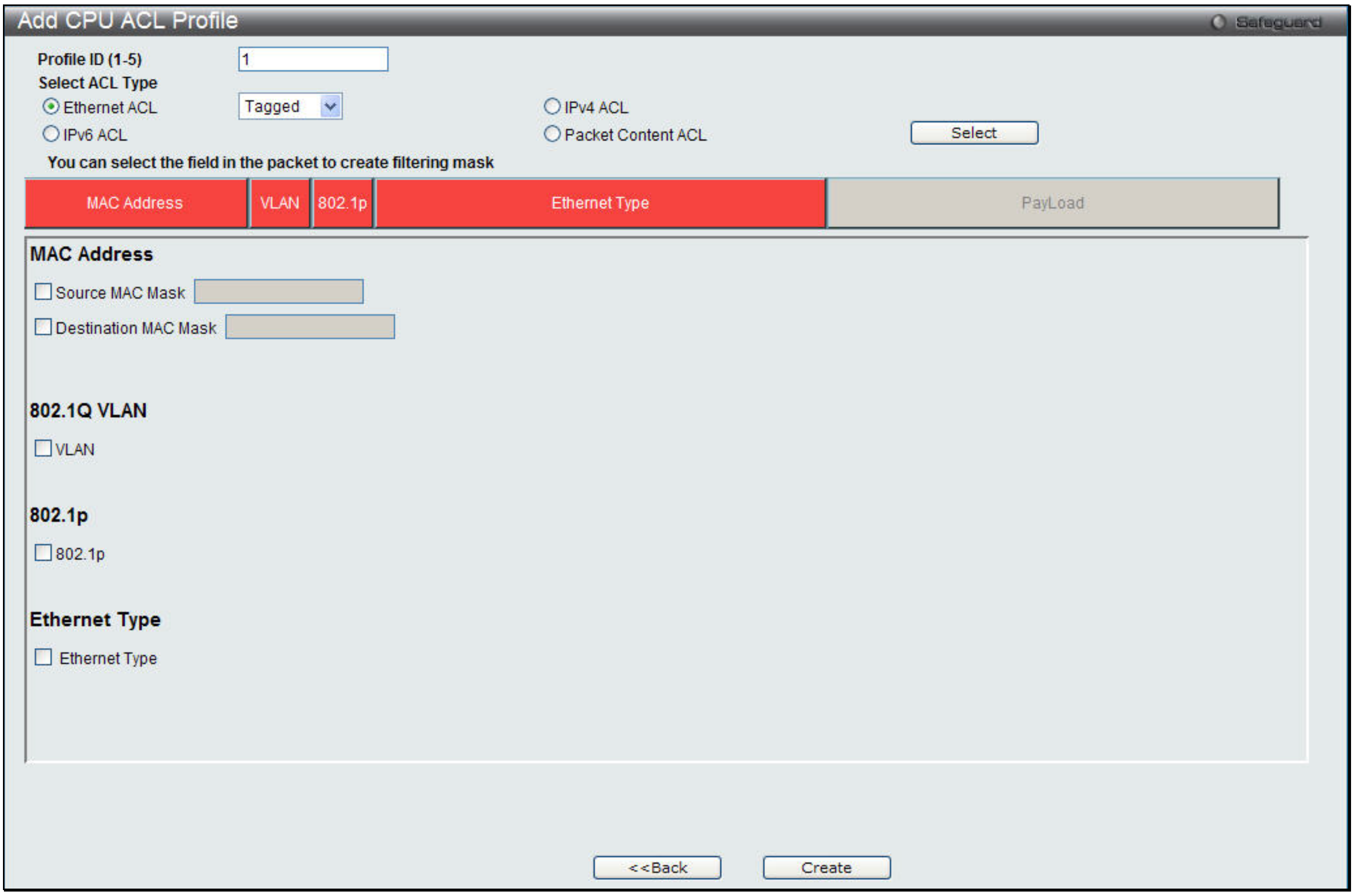
There are four **Add CPU ACL Profile** windows;

- one for Ethernet (or MAC address-based) profile configuration,
- one for IPv6 address-based profile configuration,
- one for IPv4 address-based profile configuration, and
- one for packet content profile configuration.

Adding a CPU Ethernet ACL Profile

The window shown below is the Add CPU ACL Profile window for Ethernet. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:


Add CPU ACL Profile
Safeguard
Select ACL Type
○ IPv4 ACL
○ IPv6 ACL
○ Packet Content ACL
Select
You can select the field in the packet to create filtering mask
MAC Address
VLAN
802.1p
Ethernet Type
PayLoad
MAC Address
☐ Source MAC Mask
☐ Destination MAC Mask
802.1Q VLAN
☐ VLAN
802.1p
☐ 802.1p
Ethernet Type
☐ Ethernet Type
<<Back
Create

Profile ID (1-5): 1

● Ethernet ACL: Tagged

Figure 7-24 Add CPU ACL Profile (Ethernet ACL)

The fields that can be configured are described below:

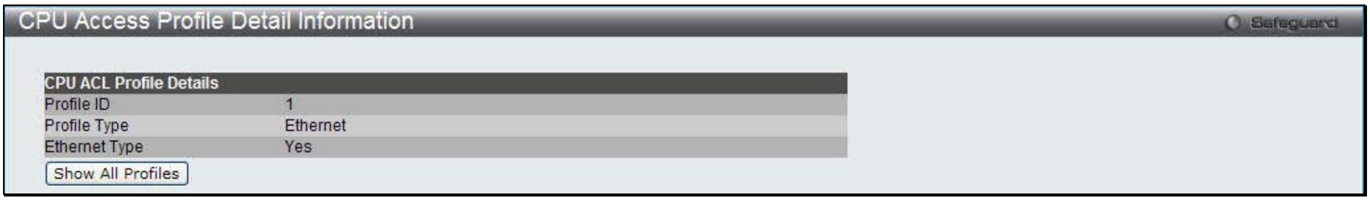
Parameter	Description
Profile ID (1-5)	Enter a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the window according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select a CPU ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:


CPU Access Profile Detail Information
Safeguard

CPU ACL Profile Details

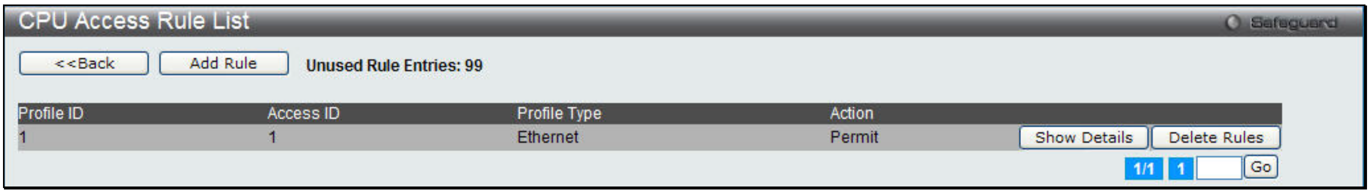
Profile ID	1
Profile Type	Ethernet
Ethernet Type	Yes

Show All Profiles

Figure 7-25 CPU Access Profile Detail Information (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:


CPU Access Rule List
Safeguard
<<Back
Add Rule

Unused Rule Entries: 99

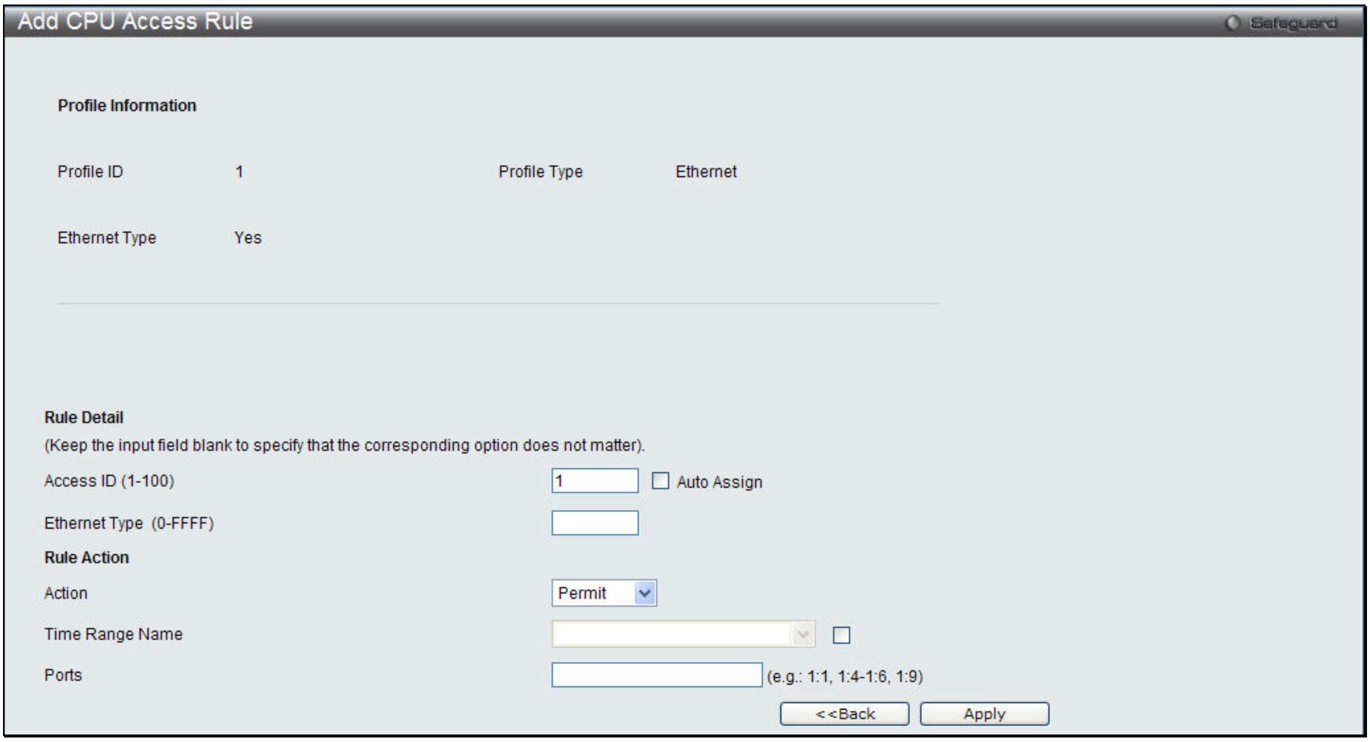
Profile ID	Access ID	Profile Type	Action	
1	1	Ethernet	Permit	Show Details Delete Rules

1/1
1
Go

Figure 7-26 CPU Access Rule List (Ethernet ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:


Add CPU Access Rule
Safeguard

Profile Information

Profile ID 1 Profile Type Ethernet

Ethernet Type Yes

Rule Detail

(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-100): 1 ☐ Auto Assign

Ethernet Type (0-FFFF):

Rule Action

Action: Permit

Time Range Name: ☐

Ports: (e.g.: 1:1, 1:4-1:6, 1:9)

<<Back
Apply

Figure 7-27 Add CPU Access Rule (Ethernet ACL)

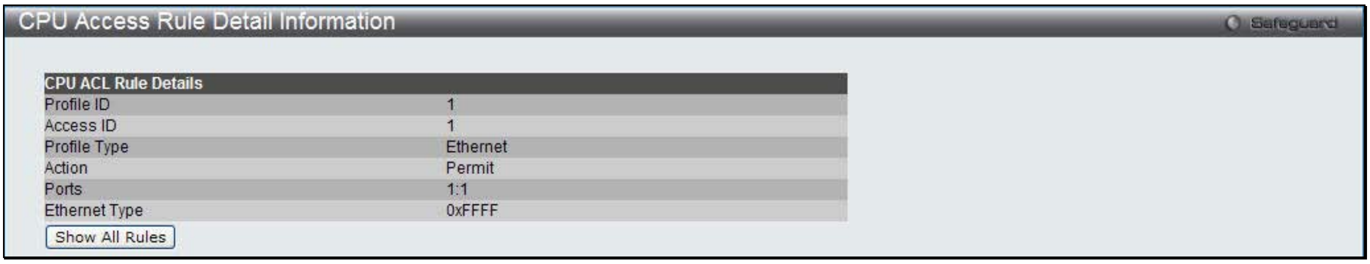
The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Ethernet Type (0-FFFF)	Enter the appropriate Ethernet Type information.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:



CPU ACL Rule Details	
Profile ID	1
Access ID	1
Profile Type	Ethernet
Action	Permit
Ports	1:1
Ethernet Type	0xFFFF

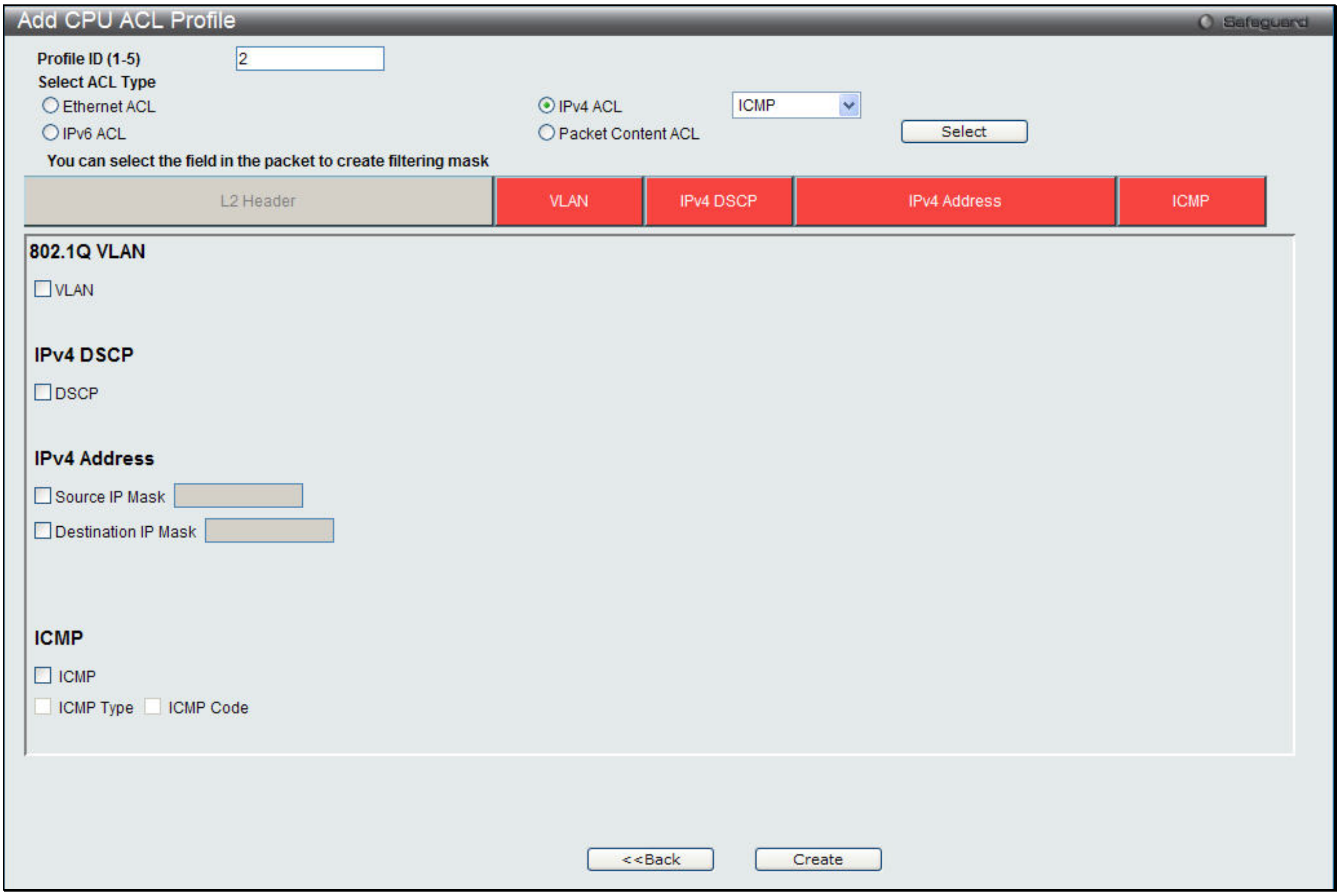
Figure 7-28 CPU Access Rule Detail Information (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU IPv4 ACL Profile

The window shown below is the **Add CPU ACL Profile** window for IP (IPv4). To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:


Add CPU ACL Profile

Profile ID (1-5): 2

Select ACL Type

○ Ethernet ACL
● IPv4 ACL: ICMP
○ IPv6 ACL
○ Packet Content ACL

You can select the field in the packet to create filtering mask

802.1Q VLAN

☐ VLAN

IPv4 DSCP

☐ DSCP

IPv4 Address

☐ Source IP Mask
☐ Destination IP Mask

ICMP

☐ ICMP
☐ ICMP Type ☐ ICMP Code

Figure 7-29 Add CPU ACL Profile (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-5)	Enter a unique identifier number for this profile set. This value can be set from *1* to *5*.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address, e.g. 255.255.255.255.
Destination IP Mask	Enter an IP address mask for the destination IP address, e.g. 255.255.255.255.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.

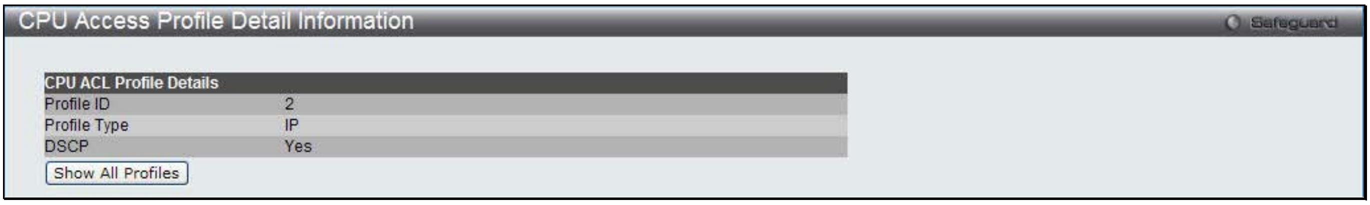
	Select *Type* to further specify that the access profile will apply an ICMP type value, or specify *Code* to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires a source port mask and/or a destination port mask is to be specified. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff). *Protocol ID Mask* – Specify that the rule applies to the IP Protocol ID Traffic. *User Define* – Specify the L4 part mask.

Click the **Select** button to select a CPU ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:



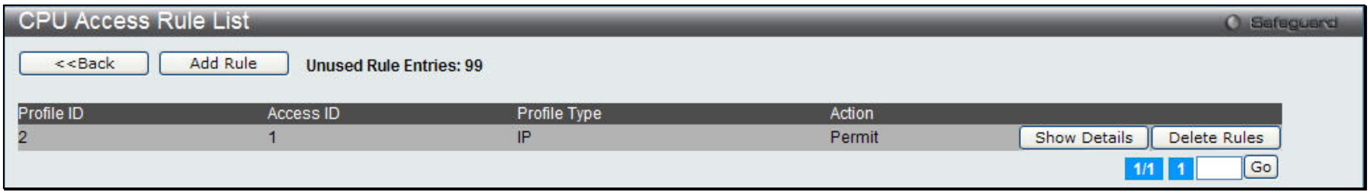
CPU Access Profile Detail Information

CPU ACL Profile Details	
Profile ID	2
Profile Type	IP
DSCP	Yes

Figure 7-30 CPU Access Profile Detail Information (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



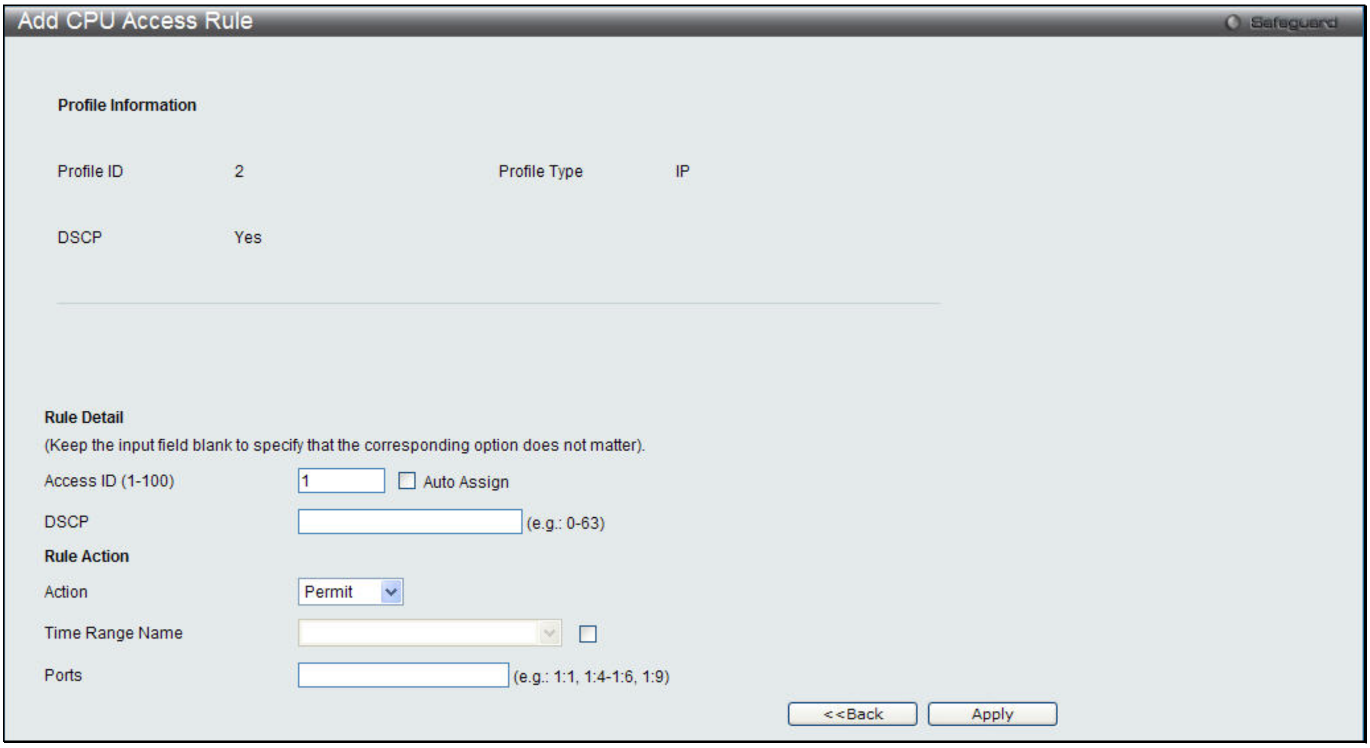
Unused Rule Entries: 99

Profile ID	Access ID	Profile Type	Action
2	1	IP	Permit

Figure 7-31 CPU Access Rule List (IPv4 ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Profile Information

Profile ID 2
Profile Type IP
DSCP Yes

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).
Access ID (1-100) 1 ☐ Auto Assign
DSCP (e.g.: 0-63)
Rule Action
Action Permit
Time Range Name ☐
Ports (e.g.: 1:1, 1:4-1:6, 1:9)

Figure 7-32 Add CPU Access Rule (IPv4 ACL)

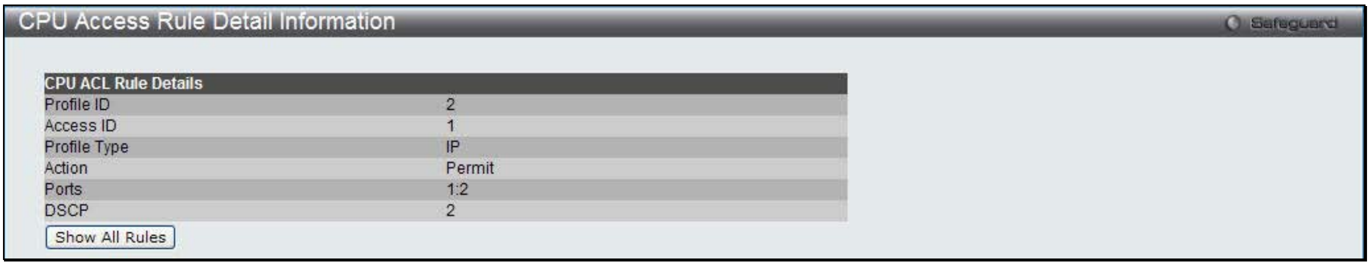
The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:


CPU Access Rule Detail Information
Safeguard
Show All Rules

CPU ACL Rule Details	
Profile ID	2
Access ID	1
Profile Type	IP
Action	Permit
Ports	1:2
DSCP	2

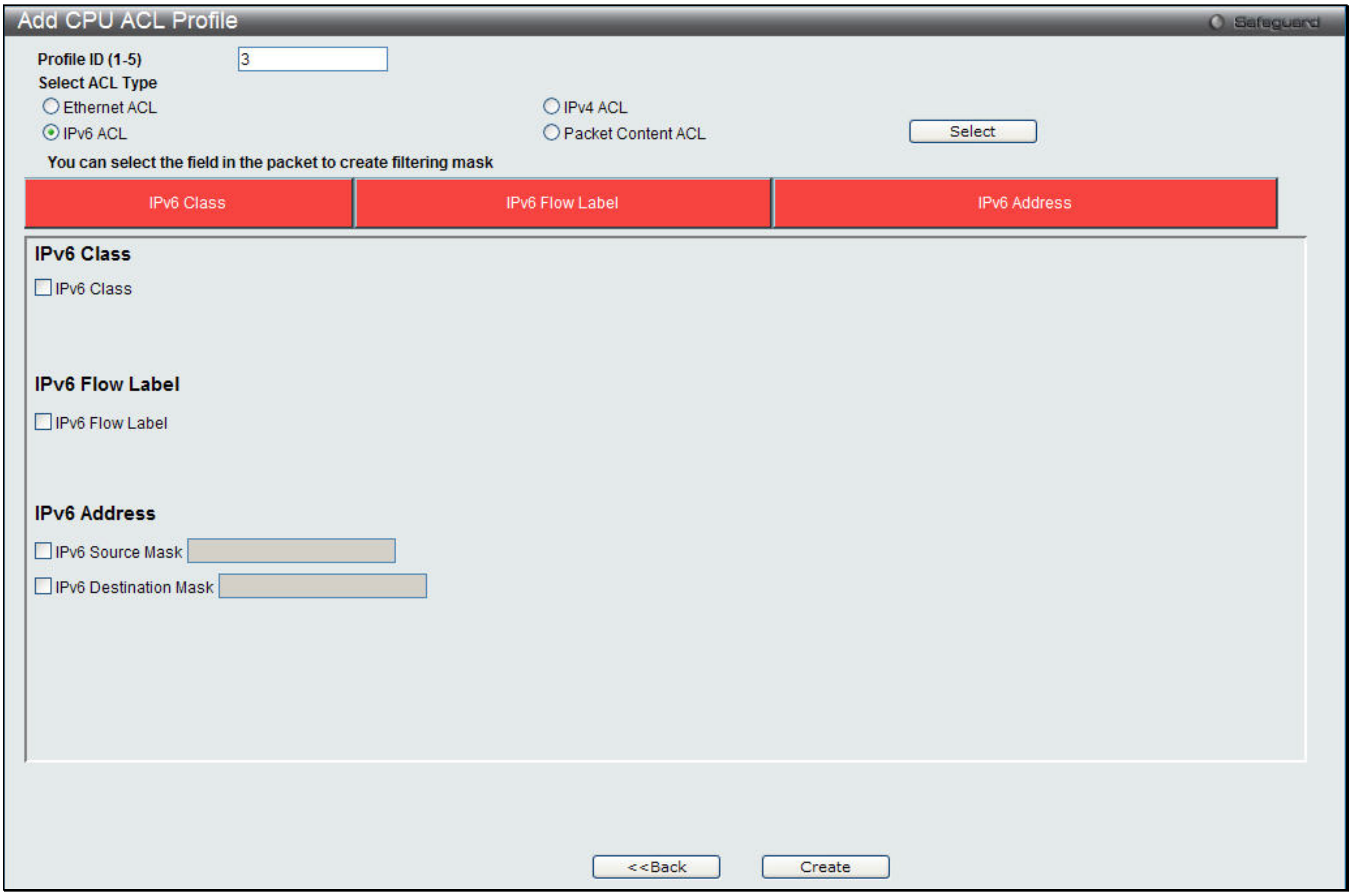
Figure 7-33 CPU Access Rule Detail Information (IPv4 ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU IPv6 ACL Profile

The window shown below is the **Add CPU ACL Profile** window for IPv6. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:


Add CPU ACL Profile
Safeguard
Select
You can select the field in the packet to create filtering mask
IPv6 Class
IPv6 Flow Label
IPv6 Address
IPv6 Class
IPv6 Flow Label
IPv6 Address
<<Back
Create

Profile ID (1-5): 3

Select ACL Type: ○ Ethernet ACL ○ IPv4 ACL ● IPv6 ACL ○ Packet Content ACL

☐ IPv6 Class

☐ IPv6 Flow Label

☐ IPv6 Source Mask

☐ IPv6 Destination Mask

Figure 7-34 Add CPU ACL Profile (IPv6 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-5)	Enter a unique identifier number for this profile set. This value can be set from *1* to*5.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or

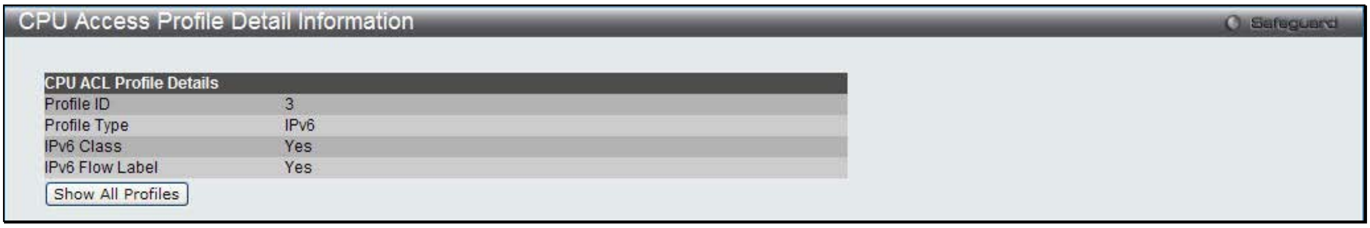
	packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
IPv6 Class	Checking this field will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 Flow Label	Checking this field will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
IPv6 Source Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
IPv6 Destination Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click the **Select** button to select a CPU ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

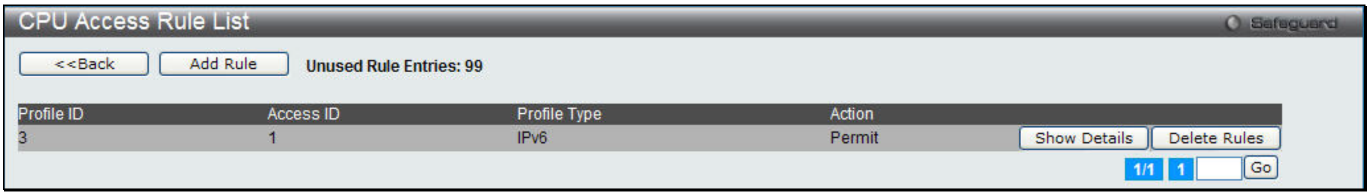


CPU ACL Profile Details	
Profile ID	3
Profile Type	IPv6
IPv6 Class	Yes
IPv6 Flow Label	Yes

Figure 7-35 CPU Access Profile Detail Information (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



Unused Rule Entries: 99

Profile ID	Access ID	Profile Type	Action	
3	1	IPv6	Permit	Show Details Delete Rules

Figure 7-36 CPU Access Rule List (IPv6 ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.

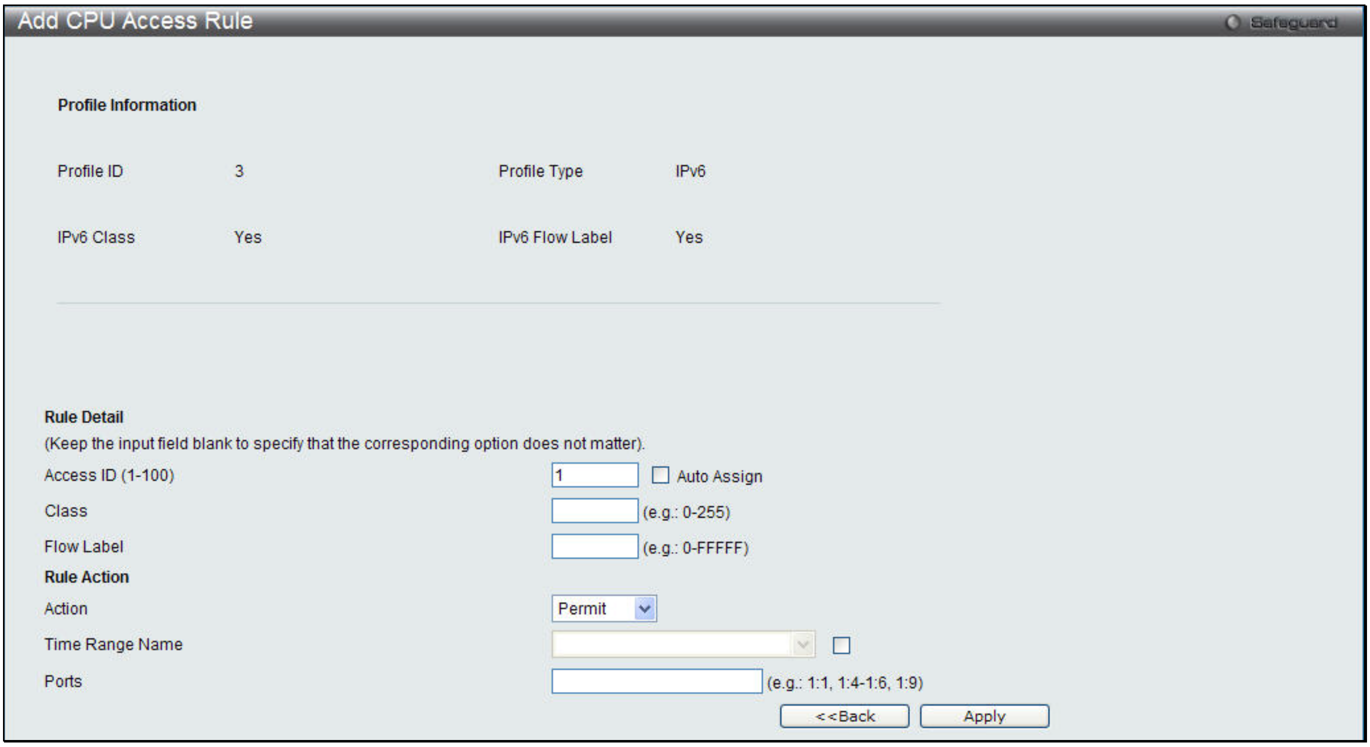
Click the **<<Back** button to return to the previous page.

Click the **Show Details** button to view more information about the specific rule created.

Click the **Delete Rules** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Add CPU Access Rule

Profile Information

Profile ID	3	Profile Type	IPv6
IPv6 Class	Yes	IPv6 Flow Label	Yes

Rule Detail

(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-100)	1 ☐ Auto Assign
Class	(e.g.: 0-255)
Flow Label	(e.g.: 0-FFFFF)

Rule Action

Action	Permit
Time Range Name	☐
Ports	(e.g.: 1:1, 1:4-1:6, 1:9)

Figure 7-37 Add CPU Access Rule (IPv6 ACL)

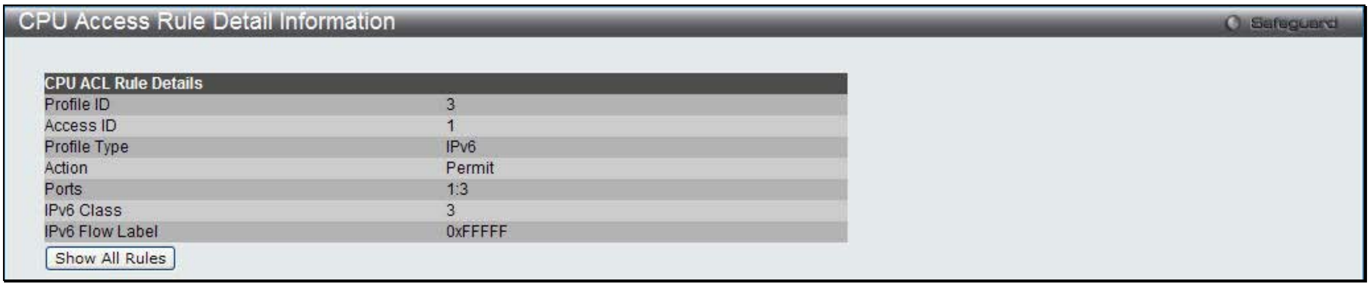
The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Enter a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:



CPU Access Rule Detail Information

CPU ACL Rule Details	
Profile ID	3
Access ID	1
Profile Type	IPv6
Action	Permit
Ports	1:3
IPv6 Class	3
IPv6 Flow Label	0xFFFFF

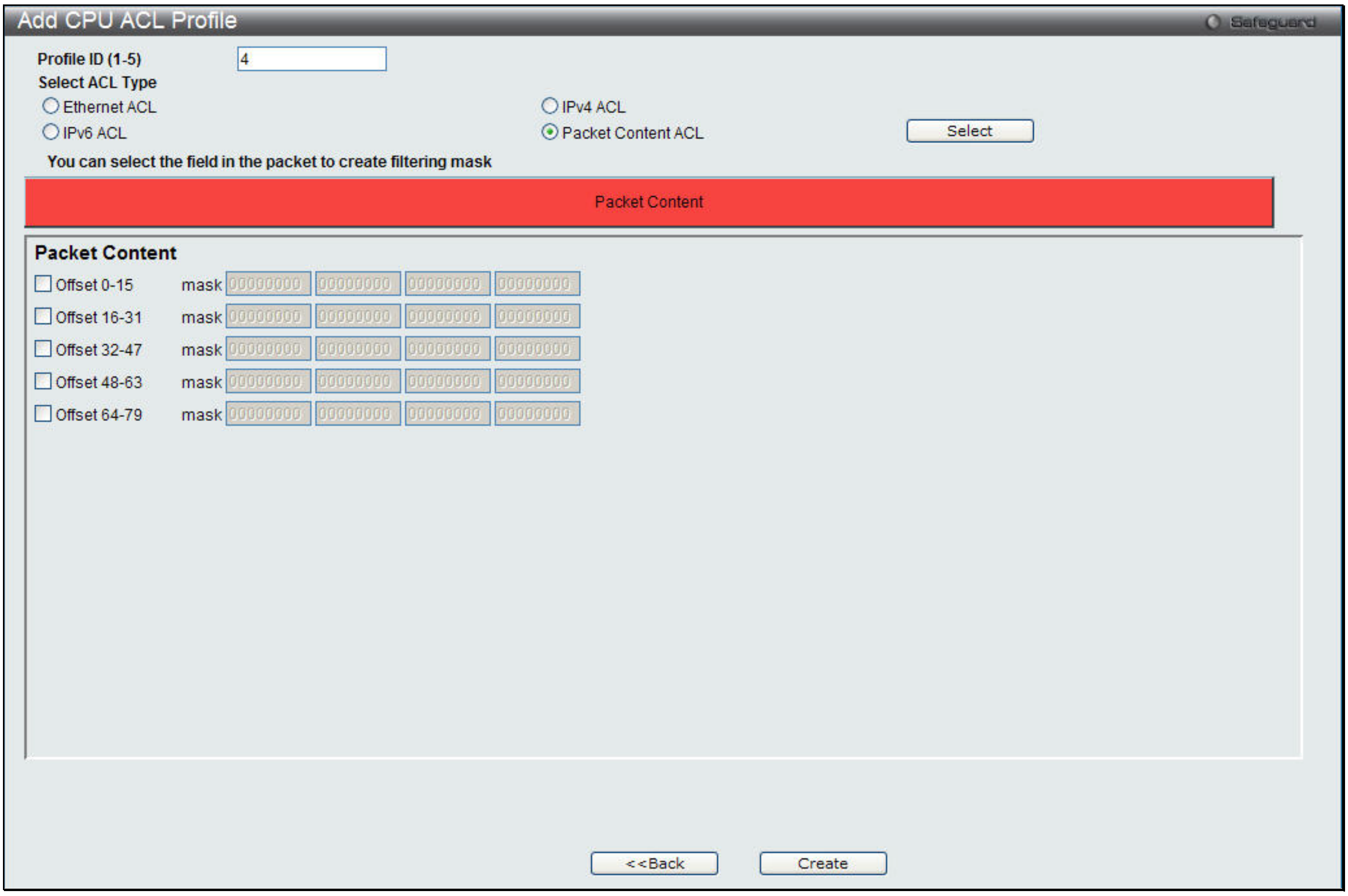
Figure 7-38 CPU Access Rule Detail Information (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

Adding a CPU Packet Content ACL Profile

The window shown below is the Add CPU ACL Profile window for Packet Content. To use specific filtering masks in this ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add CPU ACL Profile** button, the following page will appear:



Add CPU ACL Profile

Profile ID (1-5): 4

Select ACL Type

○ Ethernet ACL
○ IPv4 ACL
○ IPv6 ACL
● Packet Content ACL

You can select the field in the packet to create filtering mask

Packet Content

☐ Offset 0-15 mask 00000000 00000000 00000000 00000000
☐ Offset 16-31 mask 00000000 00000000 00000000 00000000
☐ Offset 32-47 mask 00000000 00000000 00000000 00000000
☐ Offset 48-63 mask 00000000 00000000 00000000 00000000
☐ Offset 64-79 mask 00000000 00000000 00000000 00000000

Figure 7-39 Add CPU ACL Profile (Packet Content ACL)

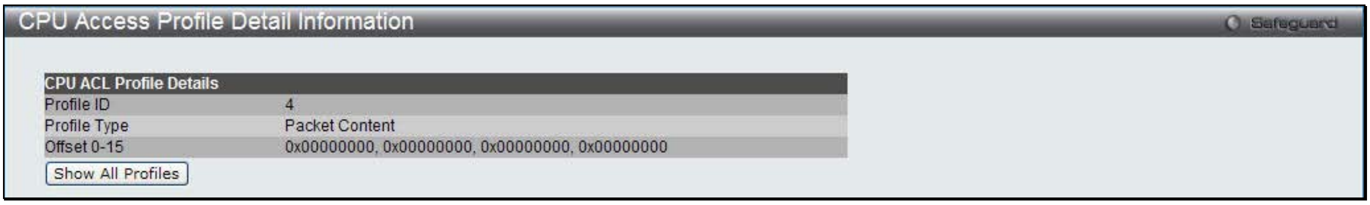
The fields that can be configured are described below:

Parameter	Description
Profile ID (1-5)	Here the user can enter a unique identifier number for this profile set. This value can be set from *1* to*5.*
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, IPv6 address, or packet content mask. This will change the menu according to the requirements for the type of profile. Select Ethernet to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 to instruct the Switch to examine the IP address in each frame's header. Select IPv6 to instruct the Switch to examine the IP address in each frame's header. Select Packet Content Mask to specify a mask to hide the content of the packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: *0-15* - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. *16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. *32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47. *48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63.

	64-79 – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click the **Select** button to select a CPU ACL type.
Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

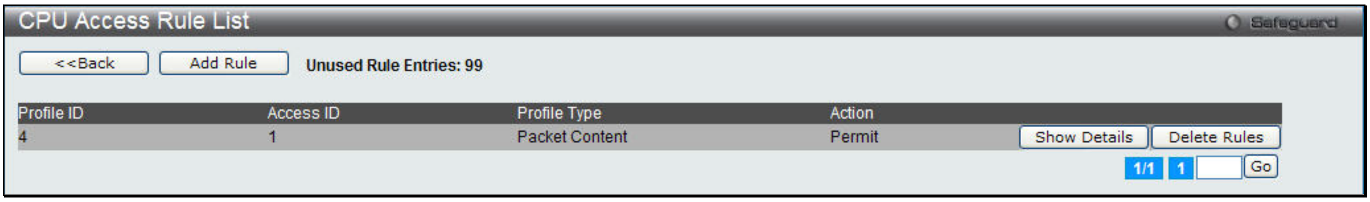


CPU ACL Profile Details	
Profile ID	4
Profile Type	Packet Content
Offset 0-15	0x00000000, 0x00000000, 0x00000000, 0x00000000

Figure 7-40 CPU Access Profile Detail Information (Packet Content ACL)

Click the **Show All Profiles** button to navigate back to the **CPU ACL Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



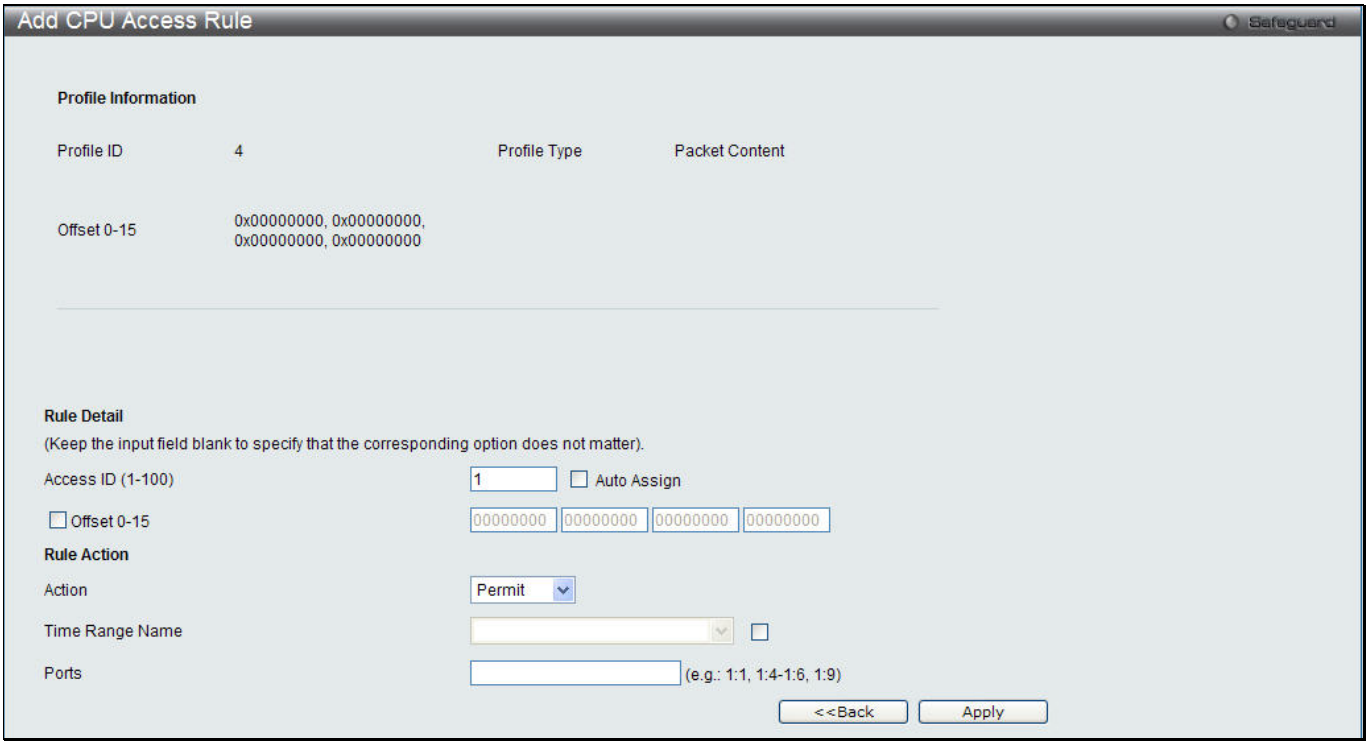
Unused Rule Entries: 99

Profile ID	Access ID	Profile Type	Action		
4	1	Packet Content	Permit	Show Details	Delete Rules

Figure 7-41 CPU Access Rule List (Packet Content ACL)

Click the **Add Rule** button to create a new CPU ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Add CPU Access Rule

Profile Information

Profile ID 4

Profile Type Packet Content

Offset 0-15 0x00000000, 0x00000000, 0x00000000, 0x00000000

Rule Detail

(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-100) 1 ☐ Auto Assign

☐ Offset 0-15 00000000 00000000 00000000 00000000

Rule Action

Action Permit

Time Range Name ☐

Ports (e.g.: 1:1, 1:4-1:6, 1:9)

Figure 7-42 Add CPU Access Rule (Packet Content ACL)

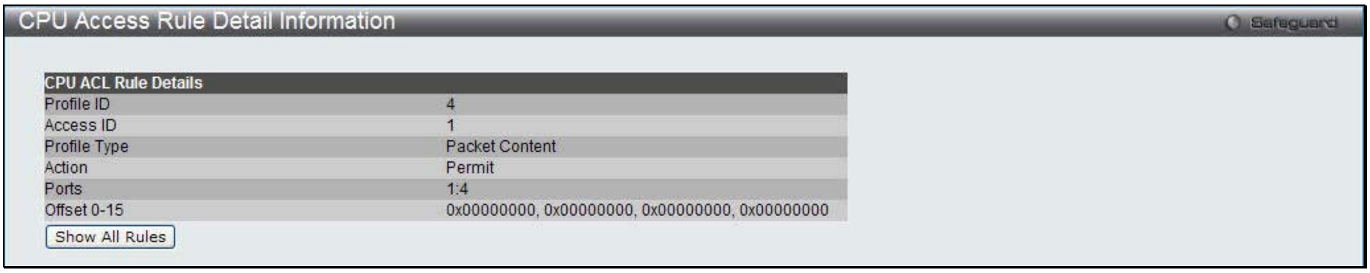
The fields that can be configured are described below:

Parameter	Description
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from *1* to *100*.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: Offset 0-15 - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. Offset 16-31 - Enter a value in hex form to mask the packet from byte 16 to byte *31.* Offset 32-47 - Enter a value in hex form to mask the packet from byte 32 to byte 47. Offset 48-63 - Enter a value in hex form to mask the packet from byte 48 to byte 63. Offset 64-79 - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Ports	Ticking the All Ports check box will denote all ports on the Switch.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **CPU Access Rule List**, the following page will appear:



CPU ACL Rule Details	
Profile ID	4
Access ID	1
Profile Type	Packet Content
Action	Permit
Ports	1:4
Offset 0-15	0x00000000, 0x00000000, 0x00000000, 0x00000000

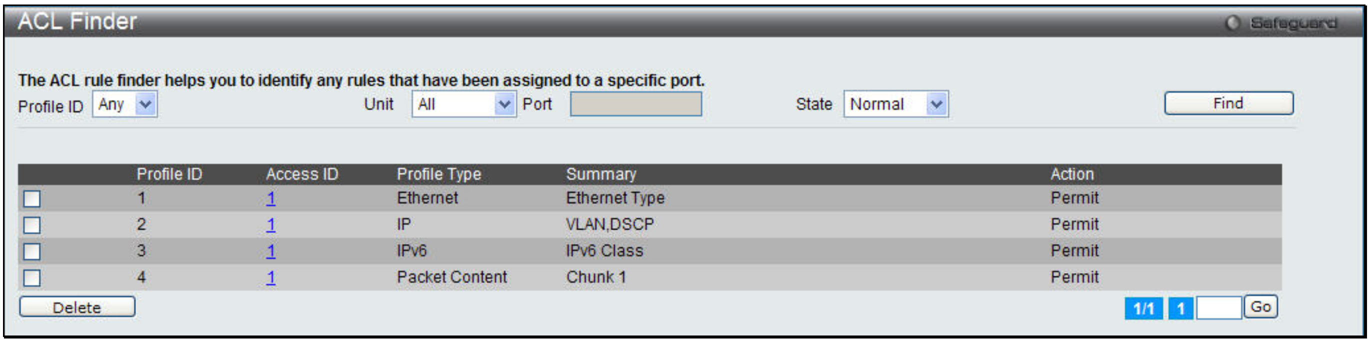
Figure 7-43 CPU Access Rule Detail Information (Packet Content ACL)

Click the **Show All Rules** button to navigate back to the CPU Access Rule List.

ACL Finder

The ACL rule finder helps you to identify any rules that have been assigned to a specific port and edit existing rules quickly.

To view this window, click **ACL > ACL Finder** as shown below:



The ACL rule finder helps you to identify any rules that have been assigned to a specific port.

Profile ID: Any
Unit: All
Port:
State: Normal

	Profile ID	Access ID	Profile Type	Summary	Action
☐	1	1	Ethernet	Ethernet Type	Permit
☐	2	1	IP	VLAN,DSCP	Permit
☐	3	1	IPv6	IPv6 Class	Permit
☐	4	1	Packet Content	Chunk 1	Permit

Figure 7-44 ACL Finder window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Use the drop-down menu to select the Profile ID for the ACL rule finder to identify the rule.
Unit	Select the unit you want to configure.
Port	Enter the port number for the ACL rule finder to identify the rule.
State	Use the drop-down menu to select the state. *Normal* - Allow the user to find normal ACL rules. *CPU* - Allow the user to find CPU ACL rules. *Egress* – Allow the user to find Egress ACL rules.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specific entry selected.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

ACL Flow Meter

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow's surpassing of two rates, the CIR and the PIR.

CIR – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn't exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

PIR – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.

PBS – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

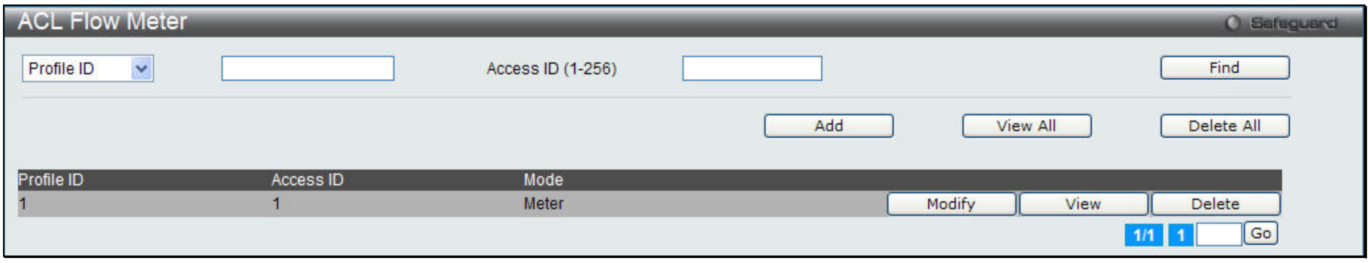
Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Violate field. Users may choose to either Permit or Drop exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the Counter check box. If the counter is enabled, the counter setting in the access profile will be disabled. Users may only enable two counters for one flow meter at any given time.

To view this window, click **ACL** > **ACL Flow Meter**, as shown below:



Profile ID	Access ID	Mode
1	1	Meter

Figure 7-45 ACL Flow Meter

The fields that can be configured are described below:

Parameter	Description
Profile ID	Use the drop-down menu to select it and enter the Profile ID for the flow meter.
Profile Name	Use the drop-down menu to select it and enter the Profile Name for the flow meter.
Access ID (1-256)	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Click the **Modify** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add** or **Modify** button, the following page will appear:

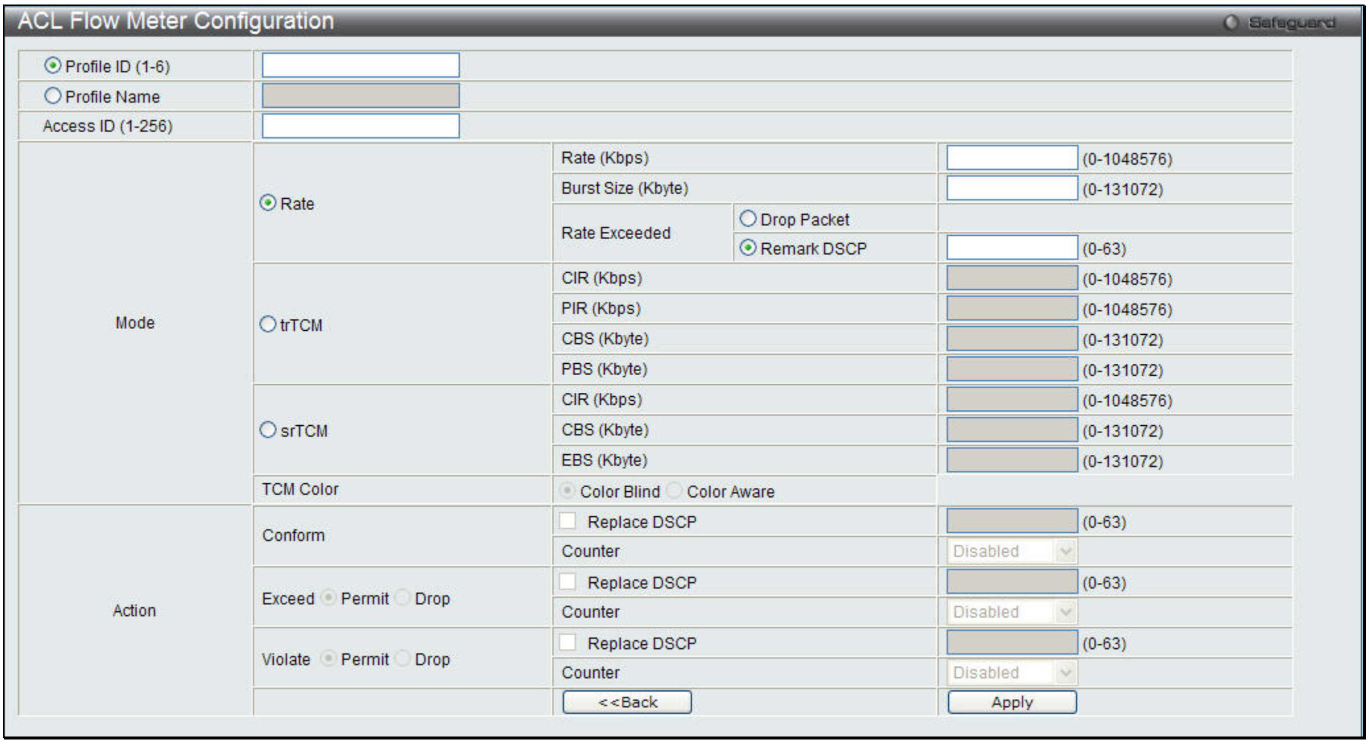

ACL Flow Meter Configuration
Safeguard
● Profile ID (1-6)
○ Profile Name
Access ID (1-256)
Mode
● Rate
Rate (Kbps) (0-1048576)
Burst Size (Kbyte) (0-131072)
Rate Exceeded
○ Drop Packet
● Remark DSCP (0-63)
○ trTCM
CIR (Kbps) (0-1048576)
PIR (Kbps) (0-1048576)
CBS (Kbyte) (0-131072)
PBS (Kbyte) (0-131072)
○ srTCM
CIR (Kbps) (0-1048576)
CBS (Kbyte) (0-131072)
EBS (Kbyte) (0-131072)
TCM Color ● Color Blind ○ Color Aware
Action
Conform
☐ Replace DSCP (0-63)
Counter Disabled
Exceed ● Permit ○ Drop
☐ Replace DSCP (0-63)
Counter Disabled
Violate ● Permit ○ Drop
☐ Replace DSCP (0-63)
Counter Disabled
<<Back
Apply

Figure 7-46 ACL Flow meter Configuration window

The fields that can be configured are described below:

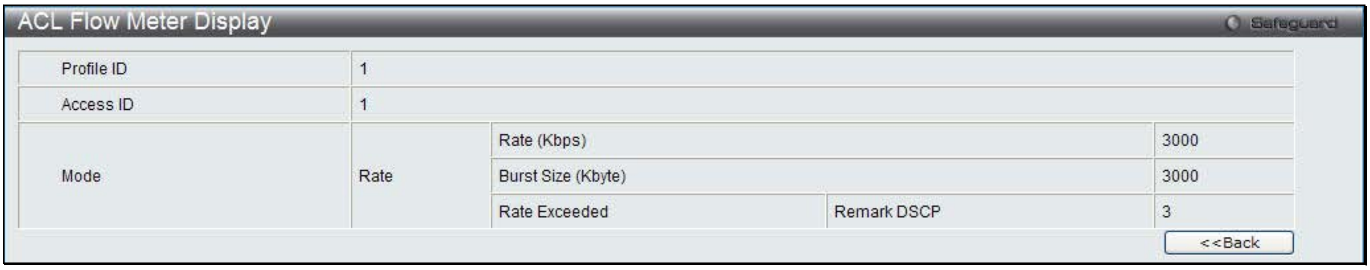
Parameter	Description
Profile ID (1-6)	Click the radio button and enter the Profile ID for the flow meter.
Profile Name	Click the radio button and enter the Profile Name for the flow meter.
Access ID (1-256)	Enter the Access ID for the flow meter.
Mode	**Rate** – Specify the rate for single rate two color mode. *Rate* – Specify the committed bandwidth in Kbps for the flow. *Burst Size* – Specify the burst size for the single rate two color mode. The unit is in kilobyte. *Rate Exceeded* – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following: *Drop Packet* – Drop the packet immediately. *Remark DSCP* – Mark the packet with a specified DSCP. The packet is set to drop for

	packets with a high precedence. **trTCM** – Specify the “two-rate three-color mode.” *CIR* – Specify the Committed information Rate. The unit is Kbps. CIR should always be equal or less than PIR. *PIR* – Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *PBS* – Specify the Peak Burst Size. The unit is in kilobyte. **srTCM** – Specify the “single-rate three-color mode”. *CIR* – Specify the Committed Information Rate. The unit is in kilobyte. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *EBS* – Specify the Excess Burst Size. The unit is in kilobyte.
Action	**Conform** – This field denotes the green packet flow. Green packet flows may have their *DSCP* field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter. *Replace DSCP* – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow. **Exceed** – This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow. **Violate** – This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

After clicking the **View** button, the following page will appear:



Profile ID	1			
Access ID	1			
Mode	Rate	Rate (Kbps)		3000
		Burst Size (Kbyte)		3000
		Rate Exceeded	Remark DSCP	3

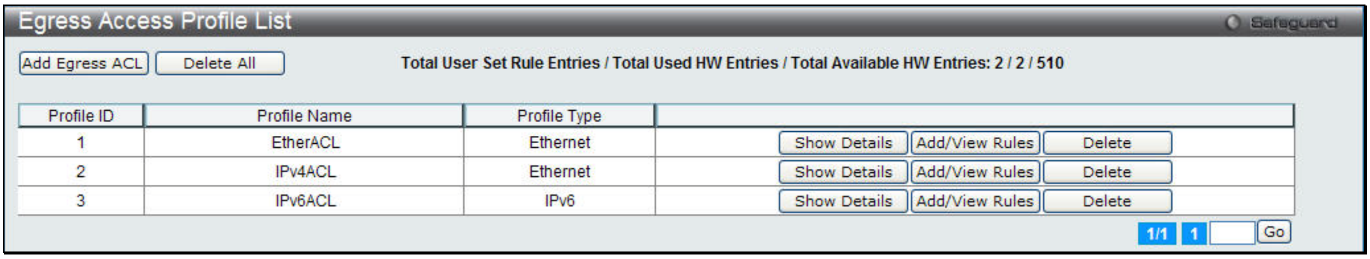
Figure 7-47 ACL Flow meter Display window

Click the **<<Back** button to return to the previous page.

Egress Access Profile List (EI Mode Only)

Egress ACL performs per-flow processing of packets when they egress the Switch. The Switch supports three Profile Types, Ethernet ACL, IPv4 ACL, and IPv6 ACL.

To view this window, click **ACL > Egress Access Profile List** as shown below:



Total User Set Rule Entries / Total Used HW Entries / Total Available HW Entries: 2 / 2 / 510

Profile ID	Profile Name	Profile Type	
1	EtherACL	Ethernet	Show Details Add/View Rules Delete
2	IPv4ACL	Ethernet	Show Details Add/View Rules Delete
3	IPv6ACL	IPv6	Show Details Add/View Rules Delete

Figure 7-48 Egress Access Profile List window

Click the **Add Egress ACL** button to add an entry to the **Egress Access Profile List**.
Click the **Delete All** button to remove all access profiles from this table.
Click the **Show Details** button to display the information of the specific profile ID entry.
Click the **Add/View Rules** button to view or add Egress ACL rules within the specified profile ID.
Click the **Delete** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

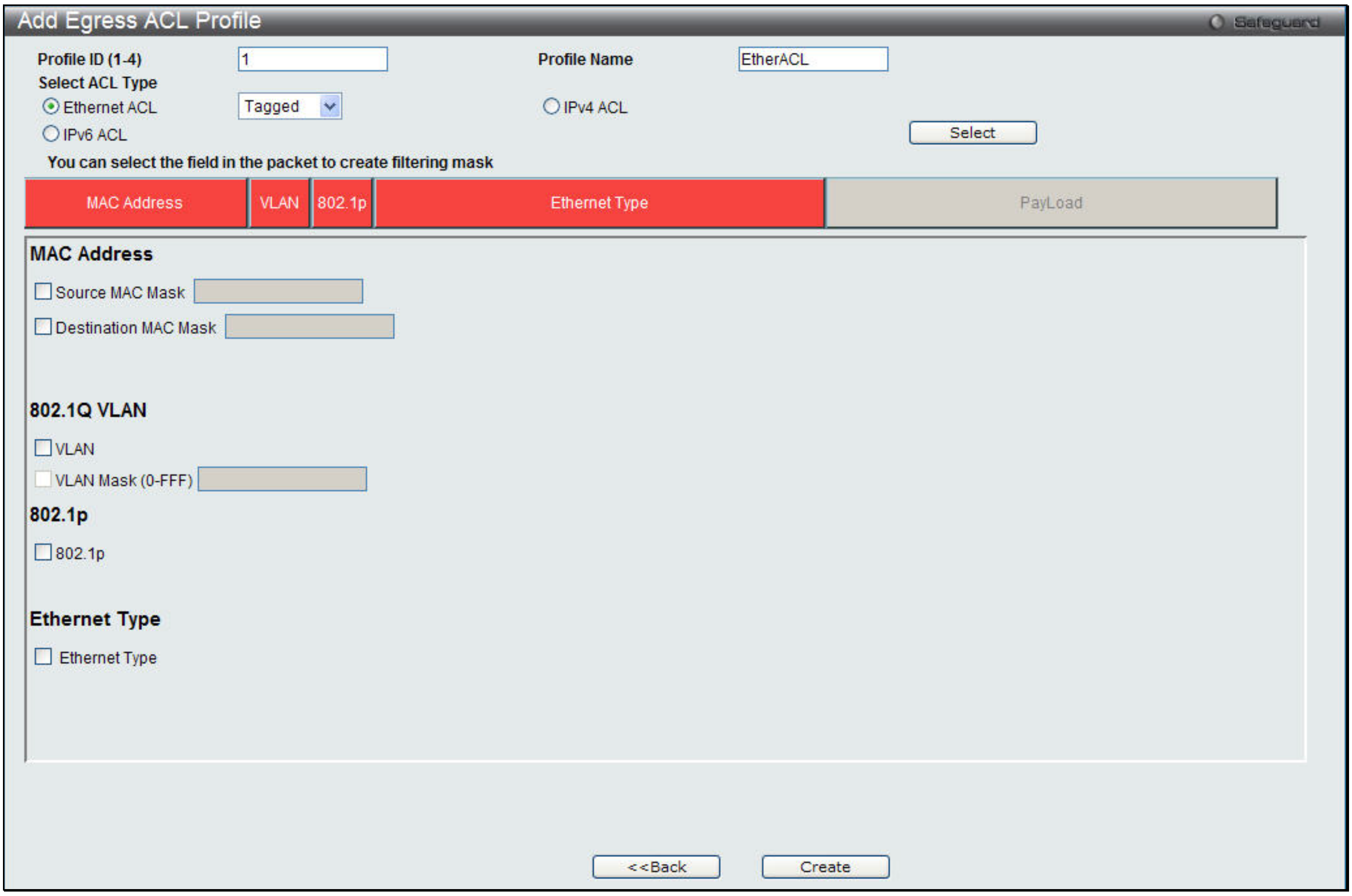
There are three **Add Egress ACL** windows;

- one for Ethernet profile configuration,
- one for IPv6 address-based profile configuration, and
- one for IPv4 address-based profile configuration.

Add an Ethernet ACL Profile

The window shown below is the Add Egress ACL Profile window for Ethernet. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add Egress ACL** button, the following page will appear:


Add Egress ACL Profile
Safeguard
You can select the field in the packet to create filtering mask
MAC Address
VLAN
802.1p
Ethernet Type
PayLoad
MAC Address
☐ Source MAC Mask
☐ Destination MAC Mask
802.1Q VLAN
☐ VLAN
☐ VLAN Mask (0-FFF)
802.1p
☐ 802.1p
Ethernet Type
☐ Ethernet Type
Select
<<Back
Create

Profile ID (1-4): 1

Profile Name: EtherACL

Select ACL Type: ● Ethernet ACL (Tagged) ○ IPv4 ACL ○ IPv6 ACL

Figure 7-49 Add Egress ACL Profile window (Ethernet ACL)

The fields that can be configured are described below:

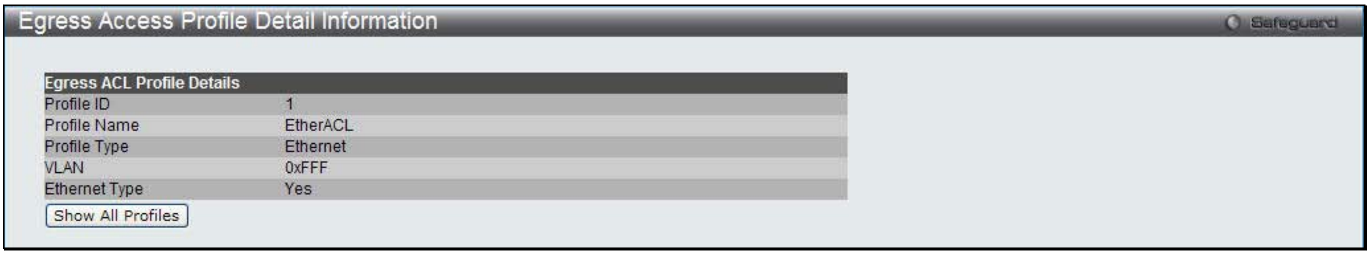
Parameter	Description
Profile ID (1-4)	Enter a unique identifier number for this profile set. This value can be set from *1* to *4.*
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
Source MAC Mask	Enter a MAC address mask for the source MAC address.
Destination MAC Mask	Enter a MAC address mask for the destination MAC address.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

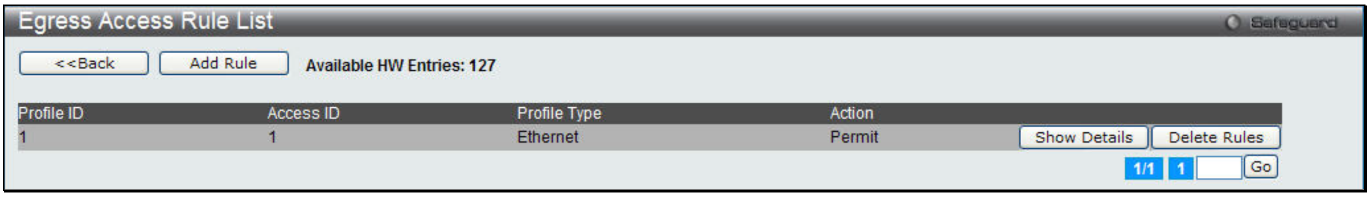

Egress Access Profile Detail Information
Safeguard
Show All Profiles

Egress ACL Profile Details	
Profile ID	1
Profile Name	EtherACL
Profile Type	Ethernet
VLAN	0xFFF
Ethernet Type	Yes

Figure 7-50 Egress Access Profile Detail Information window (Ethernet ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:


Egress Access Rule List
Safeguard
<<Back
Add Rule
Show Details
Delete Rules
1/1
1
Go

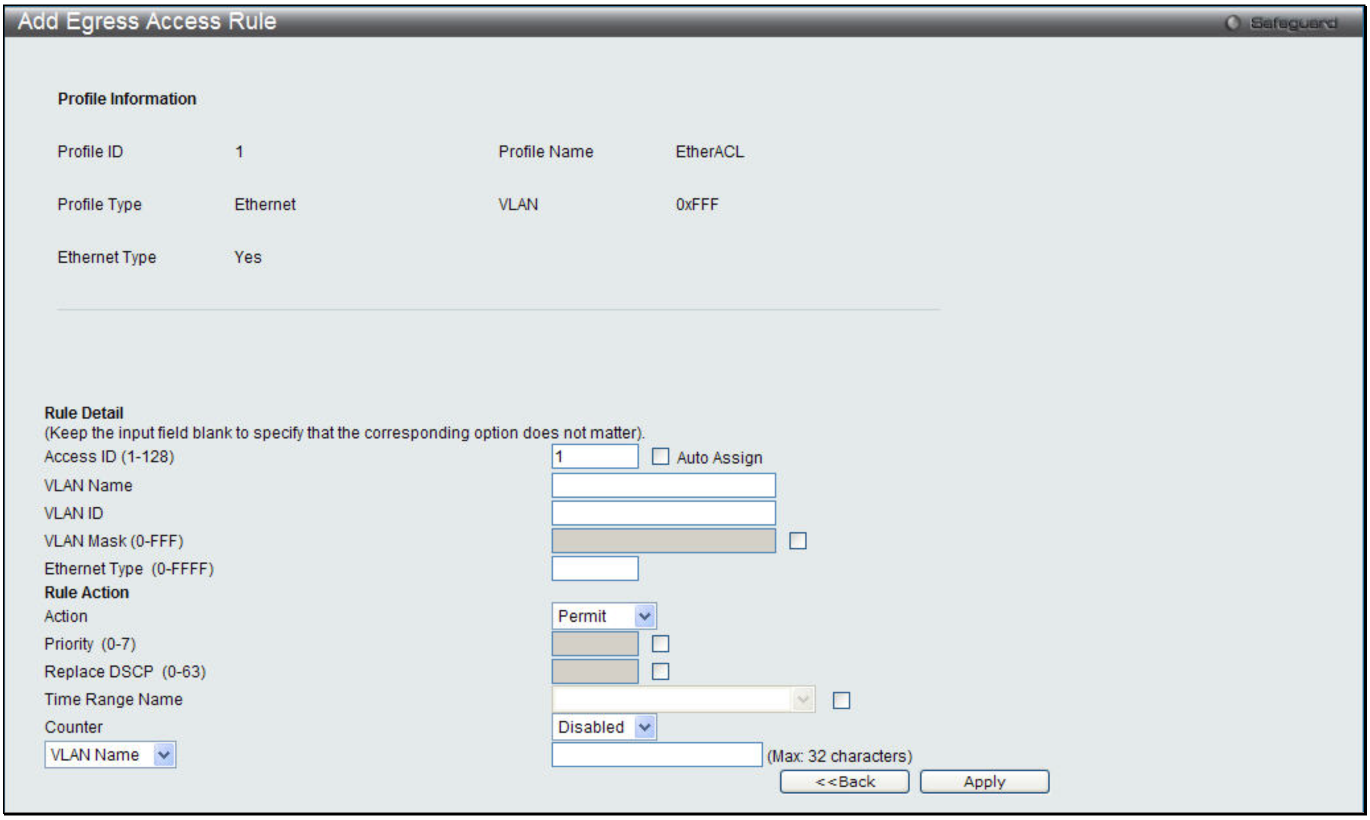
Available HW Entries: 127

Profile ID	Access ID	Profile Type	Action
1	1	Ethernet	Permit

Figure 7-51 Egress Access Rule List window (Ethernet ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:


Add Egress Access Rule
Safeguard
<<Back
Apply

Profile Information

Profile ID	1	Profile Name	EtherACL
Profile Type	Ethernet	VLAN	0xFFF
Ethernet Type	Yes		

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-128)	1 ☐ Auto Assign
VLAN Name	
VLAN ID	
VLAN Mask (0-FFF)	☐
Ethernet Type (0-FFFF)	

Rule Action

Action	Permit
Priority (0-7)	☐
Replace DSCP (0-63)	☐
Time Range Name	☐
Counter	Disabled
VLAN Name	(Max: 32 characters)

Figure 7-52 Add Egress Access Rule window (Ethernet ACL)

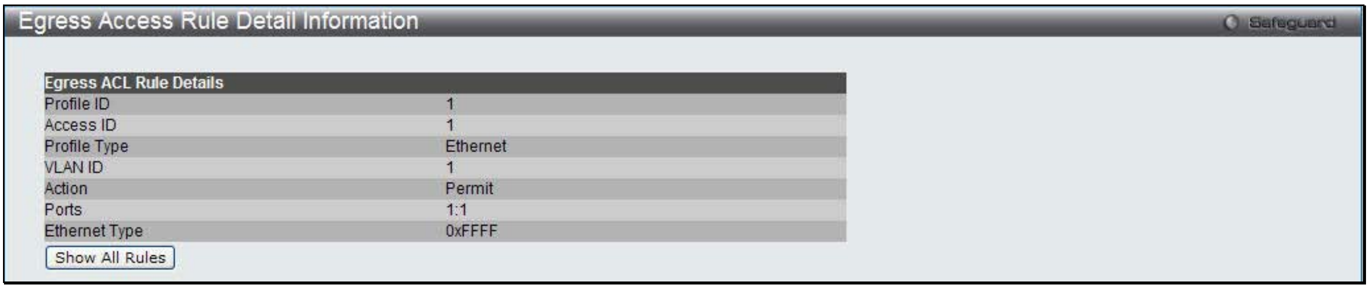
The fields that can be configured are described below:

Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. *Auto Assign* – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Ethernet Type	Specify the Ethernet type.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Port	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



Egress ACL Rule Details	
Profile ID	1
Access ID	1
Profile Type	Ethernet
VLAN ID	1
Action	Permit
Ports	1:1
Ethernet Type	0xFFFF

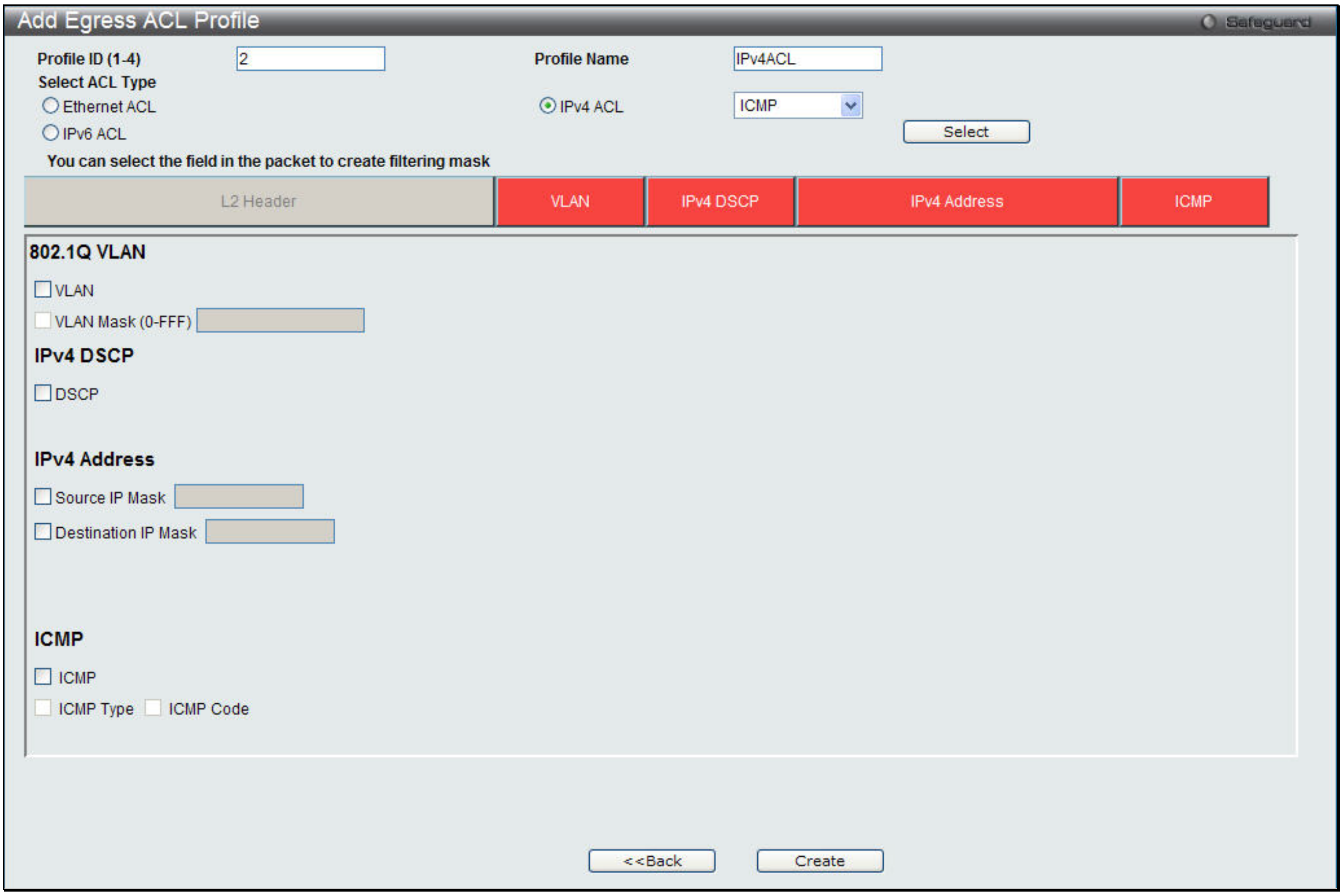
Figure 7-53 Egress Access Rule Detail Information window (Ethernet ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv4 ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv4. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add Egress ACL** button, the following page will appear:



Add Egress ACL Profile

Profile ID (1-4): 2

Profile Name: IPv4ACL

Select ACL Type: ○ Ethernet ACL ● IPv4 ACL ○ IPv6 ACL

ICMP

You can select the field in the packet to create filtering mask

Figure 7-54 Add Egress ACL Profile window (IPv4 ACL)

The fields that can be configured are described below:

Parameter	Description
Profile ID (1-4)	Enter a unique identifier number for this profile set. This value can be set from *1* to *4.*
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
802.1Q VLAN	Selecting this option instructs the Switch to examine the 802.1Q VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
IPv4 DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
IPv4 Source IP Mask	Enter an IP address mask for the source IP address.
IPv4 Destination IP	Enter an IP address mask for the destination IP address.

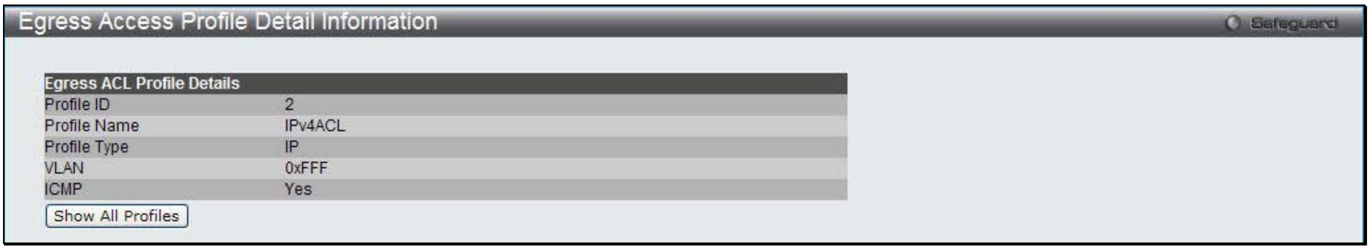
Mask	
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header. Select *Type* to further specify that the access profile will apply an IGMP type value. Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. *dst port mask* - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. *flag bit* - The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask. *src port mask* - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). *dst port mask* - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). Select *Protocol ID* - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff. *Protocol ID Mask* - Specify that the rule applies to the IP protocol ID traffic. *User Define* - Specify the Layer 4 part mask

Click the **Select** button to select an ACL type.

Click the **Create** button to create a profile.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

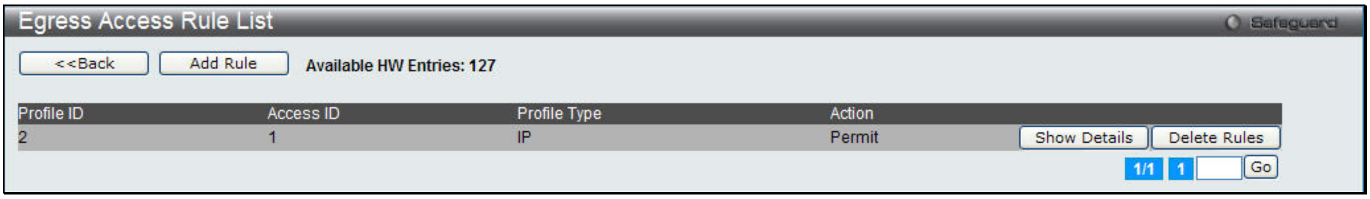


Egress ACL Profile Details	
Profile ID	2
Profile Name	IPv4ACL
Profile Type	IP
VLAN	0xFFF
ICMP	Yes

Figure 7-55 Egress Access Profile Detail Information window (IPv4 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



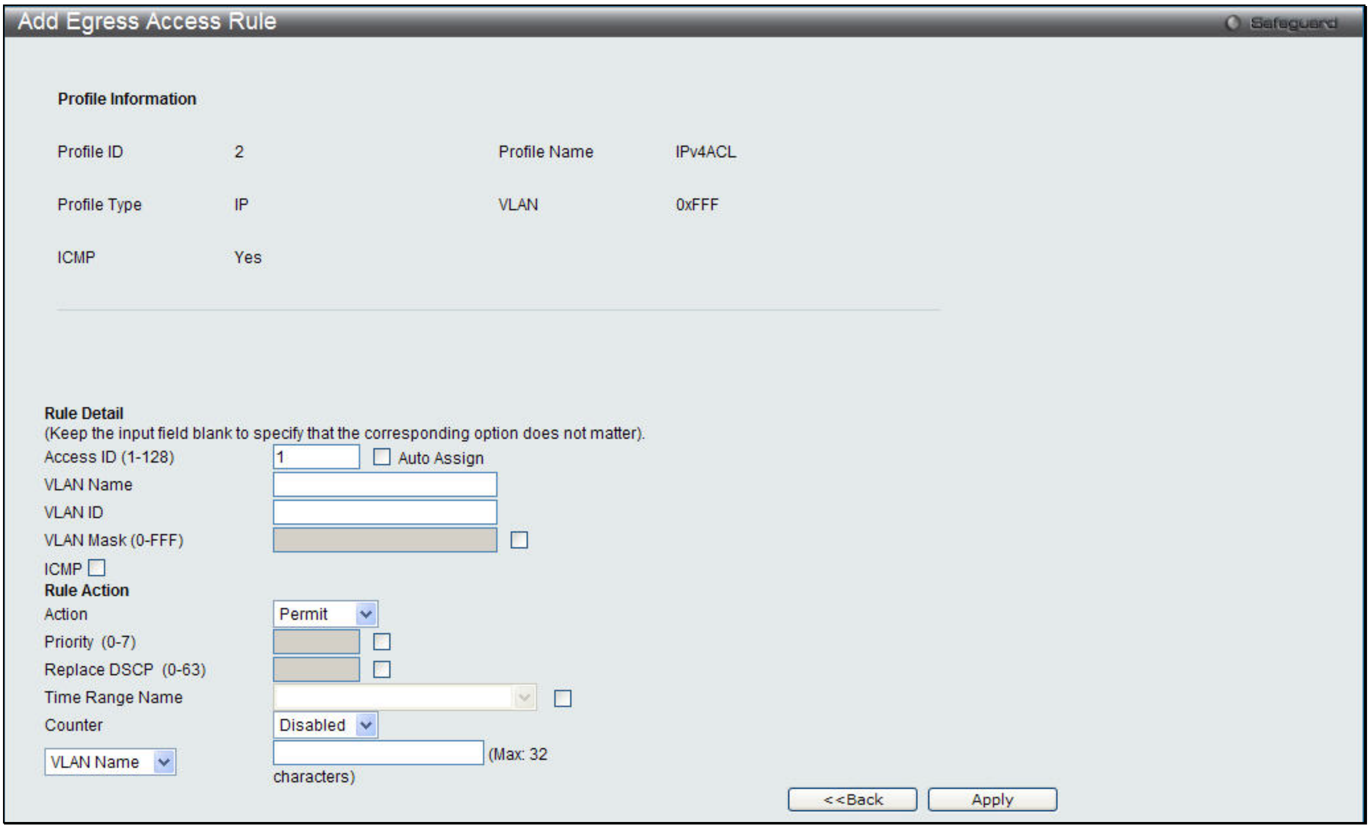
Available HW Entries: 127

Profile ID	Access ID	Profile Type	Action
2	1	IP	Permit

Figure 7-56 Egress Access Rule List window (IPv4 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Profile Information

Profile ID	2	Profile Name	IPv4ACL
Profile Type	IP	VLAN	0xFFF
ICMP	Yes		

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-128) 1 ☐ Auto Assign
VLAN Name
VLAN ID
VLAN Mask (0-FFF) ☐
ICMP ☐

Rule Action
Action Permit
Priority (0-7) ☐
Replace DSCP (0-63) ☐
Time Range Name ☐
Counter Disabled
VLAN Name (Max: 32 characters)

Figure 7-57 Add Egress Access Rule (IPv4 ACL)

The fields that can be configured are described below:

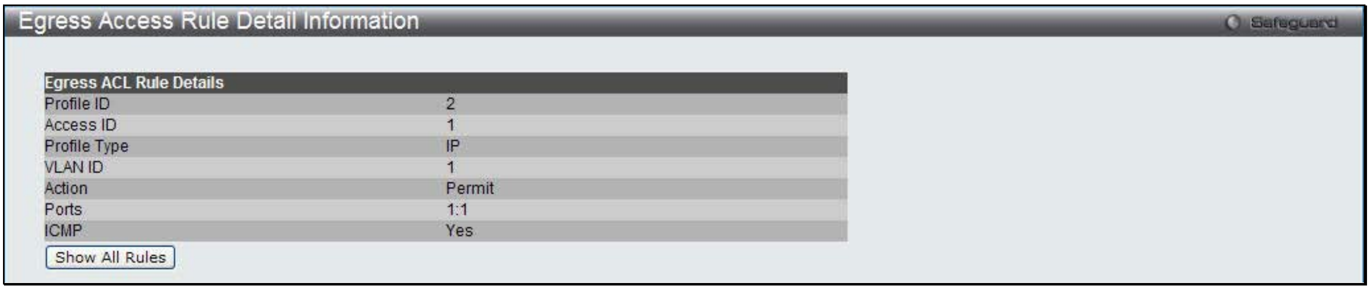
Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
DSCP	Specify the value of DSCP. The DSCP value ranges from 0 to 63.
Action	Select Permit to specify that the packets that match the access profile are forwarded

	by the Switch, according to any additional rule added (see below). Select Deny to specify that the packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv4 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:



Egress ACL Rule Details	
Profile ID	2
Access ID	1
Profile Type	IP
VLAN ID	1
Action	Permit
Ports	1:1
ICMP	Yes

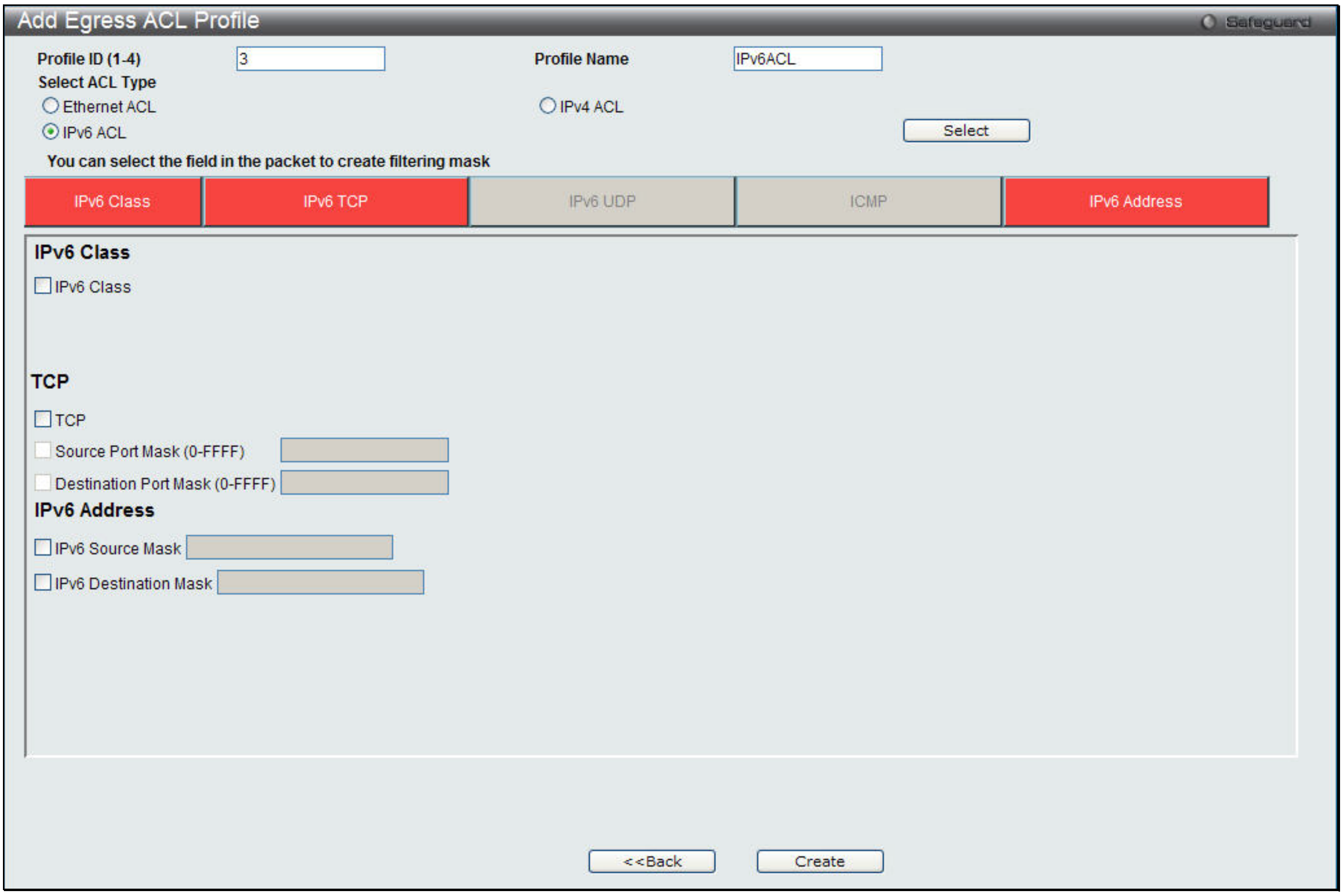
Figure 7-58 Egress Access Rule Detail Information (IPv4 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Adding an IPv6 ACL Profile

The window shown below is the Add Egress ACL Profile window for IPv6. To use specific filtering masks in this egress ACL profile, click the packet filtering mask field to highlight it red. This will add more filed to the mask.

After clicking the **Add Egress ACL** button, the following page will appear:



Add Egress ACL Profile

Profile ID (1-4): 3

Profile Name: IPv6ACL

Select ACL Type

○ Ethernet ACL

○ IPv4 ACL

● IPv6 ACL

You can select the field in the packet to create filtering mask

IPv6 Class

☐ IPv6 Class

TCP

☐ TCP

☐ Source Port Mask (0-FFFF)

☐ Destination Port Mask (0-FFFF)

IPv6 Address

☐ IPv6 Source Mask

☐ IPv6 Destination Mask

Figure 7-59 Add Egress ACL Profile window (IPv6 ACL)

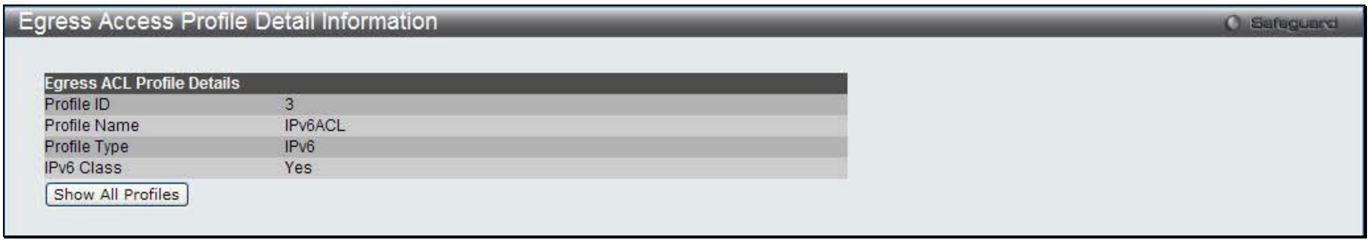
The fields that can be configured are described below:

Parameter	Description
Profile ID (1-4)	Enter a unique identifier number for this profile set. This value can be set from *1* to *4.*
Profile Name	Enter a profile name for the profile created.
Select ACL Type	Select profile based on Ethernet (MAC Address), IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile. Select Ethernet ACL to instruct the Switch to examine the layer 2 part of each packet header. Select IPv4 ACL to instruct the Switch to examine the IPv4 address in each frame's header. Select IPv6 ACL to instruct the Switch to examine the IPv6 address in each frame's header.
IPv6 Class	Ticking this check box will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
IPv6 TCP	*Source Port Mask* – Specify that the rule applies to the range of TCP source ports. *Destination Port Mask* – Specify the range of the TCP destination port range.
IPv6 UDP	*Source Port Mask* – Specify the range of the UDP source port range. *Destination Port Mask* – Specify the range of the UDP destination port mask.
ICMP	Select *ICMP* to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.
IPv6 Source Mask	The user may specify an IP address mask for the source IPv6 address by ticking the corresponding check box and entering the IP address mask, e.g.

	255.255.255.255.
IPv6 Destination Mask	The user may specify an IP address mask for the destination IPv6 address by ticking the corresponding check box and entering the IP address mask, e.g. 255.255.255.255.

Click the **Select** button to select an ACL type.
Click the **Create** button to create a profile.
Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button, the following page will appear:

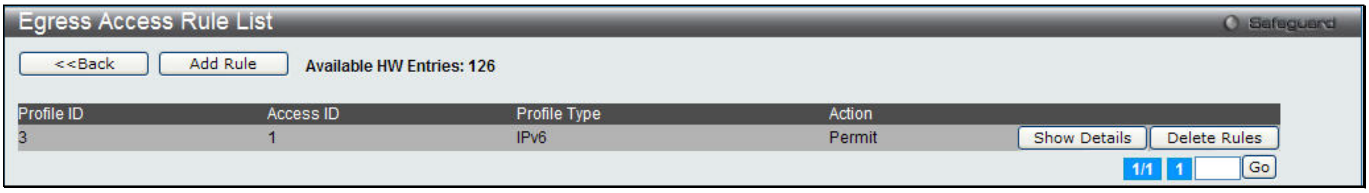


Egress ACL Profile Details	
Profile ID	3
Profile Name	IPv6ACL
Profile Type	IPv6
IPv6 Class	Yes

Figure 7-60 Egress Access Profile Detail Information window (IPv6 ACL)

Click the **Show All Profiles** button to navigate back to the **Access Profile List** Page.

After clicking the **Add/View Rules** button, the following page will appear:



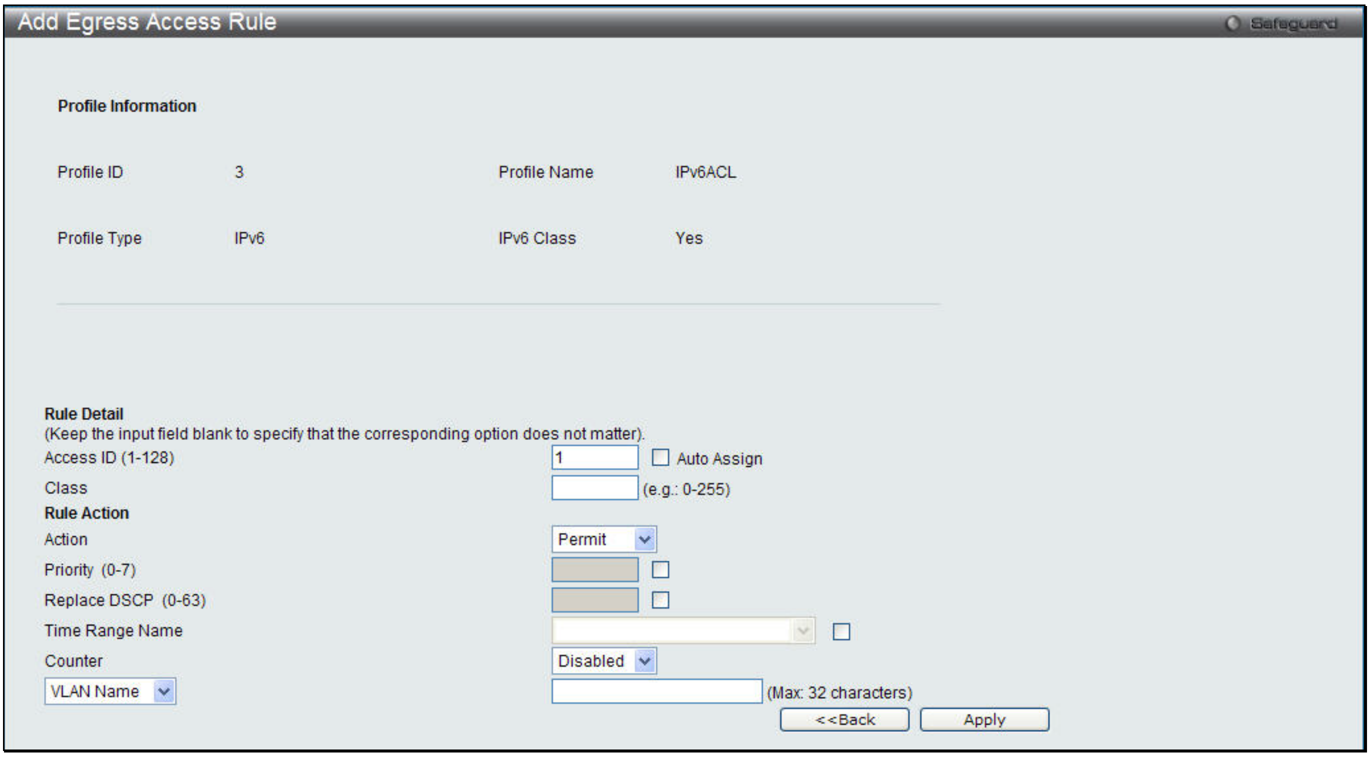
Available HW Entries: 126

Profile ID	Access ID	Profile Type	Action
3	1	IPv6	Permit

Figure 7-61 Egress Access Rule List window (IPv6 ACL)

Click the **Add Rule** button to create a new ACL rule in this profile.
Click the **<<Back** button to return to the previous page.
Click the **Show Details** button to view more information about the specific rule created.
Click the **Delete Rules** button to remove the specific entry.
Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

After clicking the **Add Rule** button, the following page will appear:



Profile ID: 3
Profile Name: IPv6ACL
Profile Type: IPv6
IPv6 Class: Yes

(Keep the input field blank to specify that the corresponding option does not matter).
Access ID (1-128): 1 ☐ Auto Assign
Class:
Action: Permit
Priority (0-7): ☐
Replace DSCP (0-63): ☐
Time Range Name: ☐
Counter: Disabled
VLAN Name:

Figure 7-62 Add Egress Access Rule (IPv6 ACL)

The fields that can be configured are described below:

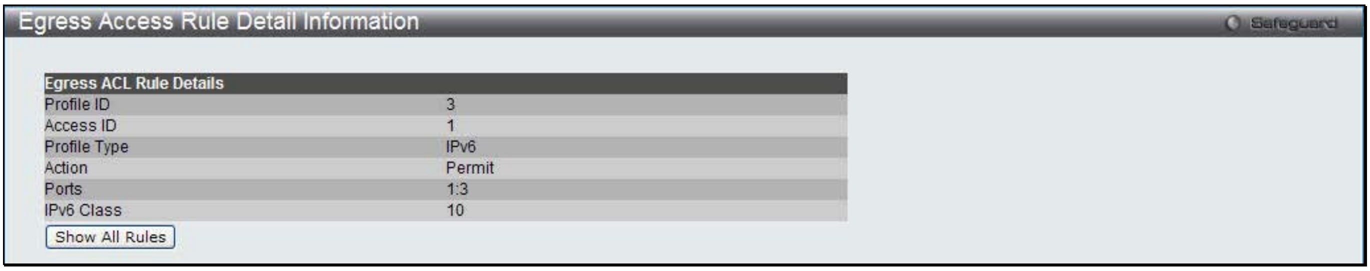
Parameter	Description
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from *1* to *128*. Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Class	Specify the value of IPv6 class.
Action	Select *Permit* to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select *Deny* to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Priority (0-7)	Tick the corresponding check box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field. When an ACL rule is added to change both the priority and DSCP of an IPv6 packet, only one of them can be modified due to a chip limitation. Currently the priority is changed when both the priority and DSCP are set to be modified.
Time Range Name	Tick the check box and enter the name of the Time Range settings that has been previously configured in the **Time Range Settings** window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Here the user can select the counter. By checking the counter, the administrator can see how many times that the rule was hit.
Ports	When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an

	error message and the access rule will not be configured. Ticking the All Ports check box will denote all ports on the Switch.
Port Group ID	Specify the port group ID to apply to the access rule.
Port Group Name	Specify the port group name to apply to the access rule.
VLAN Name	Specify the VLAN name to apply to the access rule.
VLAN ID	Specify the VLAN ID to apply to the access rule.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Show Details** button in the **Access Rule List**, the following page will appear:


Egress Access Rule Detail Information
Safeguard
Show All Rules

Egress ACL Rule Details	
Profile ID	3
Access ID	1
Profile Type	IPv6
Action	Permit
Ports	1:3
IPv6 Class	10

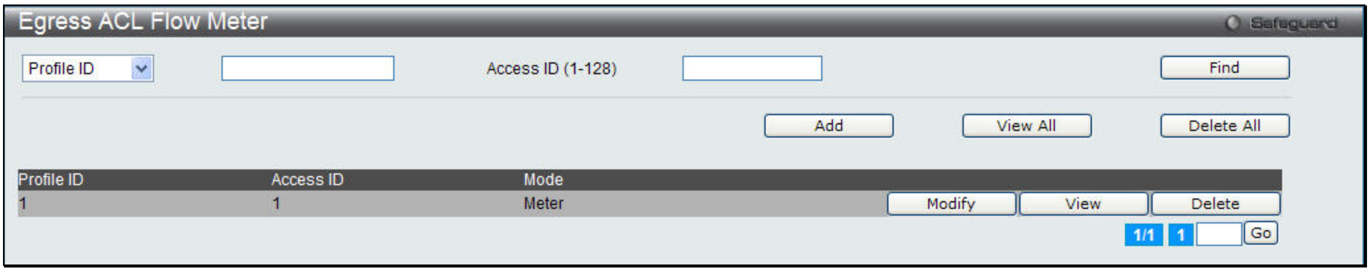
Figure 7-63 Egress Access Rule Detail Information (IPv6 ACL)

Click the **Show All Rules** button to navigate back to the Access Rule List.

Egress ACL Flow Meter (EI Mode Only)

This window is used to configure the packet flow-based metering based on an egress access profile and rule.

To view this window, click **ACL > Egress ACL Flow Meter** as shown below:


Egress ACL Flow Meter
Safeguard
Profile ID
Access ID (1-128)
Find
Add
View All
Delete All
Modify
View
Delete
1/1
1
Go

Profile ID	Access ID	Mode
1	1	Meter

Figure 7-64 Egress ACL Flow Meter window

The fields that can be configured are described below:

Parameter	Description
Profile ID	Use the drop-down menu to select it and enter the Profile ID for the flow meter.
Profile Name	Use the drop-down menu to select it and enter the Profile Name for the flow meter.
Access ID (1-128)	Here the user can enter the Access ID for the flow meter.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add** button to add a new entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

Click the **Modify** button to re-configure the specific entry.

Click the **View** button to display the information of the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Add** or **Modify** button, the following page will appear:

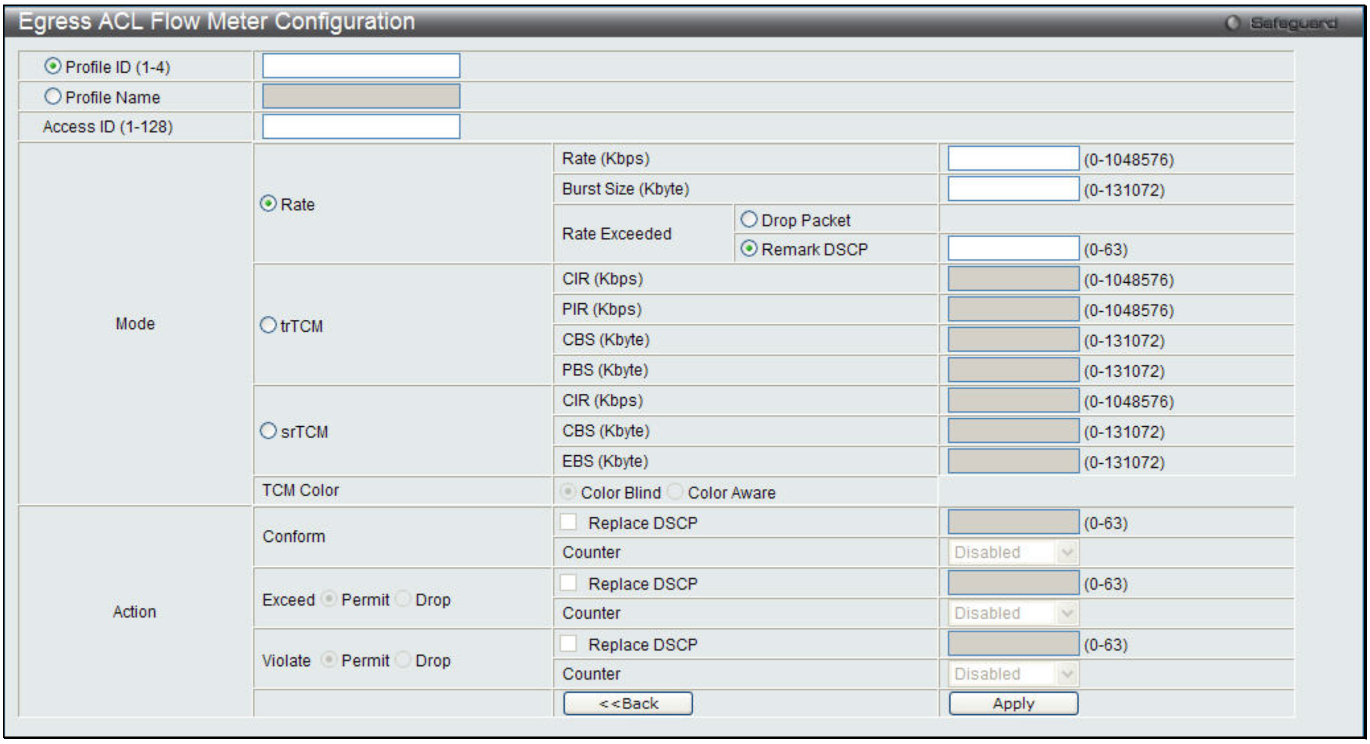

Egress ACL Flow Meter Configuration
Safeguard
● Profile ID (1-4)
○ Profile Name
Access ID (1-128)
Mode
● Rate
Rate (Kbps) (0-1048576)
Burst Size (Kbyte) (0-131072)
Rate Exceeded
○ Drop Packet
● Remark DSCP (0-63)
○ trTCM
CIR (Kbps) (0-1048576)
PIR (Kbps) (0-1048576)
CBS (Kbyte) (0-131072)
PBS (Kbyte) (0-131072)
○ srTCM
CIR (Kbps) (0-1048576)
CBS (Kbyte) (0-131072)
EBS (Kbyte) (0-131072)
TCM Color ● Color Blind ○ Color Aware
Action
Conform
☐ Replace DSCP (0-63)
Counter Disabled
Exceed ● Permit ○ Drop
☐ Replace DSCP (0-63)
Counter Disabled
Violate ● Permit ○ Drop
☐ Replace DSCP (0-63)
Counter Disabled
<<Back
Apply

Figure 7-65 Egress ACL Flow Meter Configuration window

The fields that can be configured are described below:

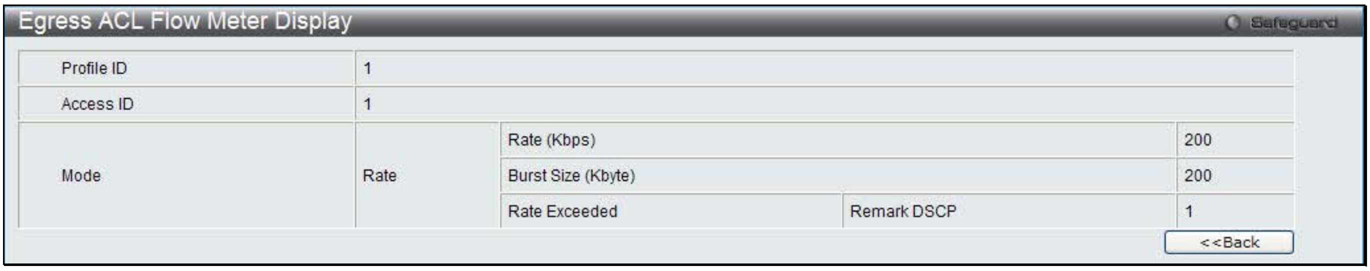
Parameter	Description
Profile ID (1-4)	Here the user can enter the Profile ID for the flow meter.
Profile Name	Here the user can enter the Profile Name for the flow meter.
Access ID (1-128)	Here the user can enter the Access ID for the flow meter.
Mode	**Rate** – Specify the rate for single rate two color mode. *Rate* – Specify the committed bandwidth in Kbps for the flow. *Burst Size* – Specify the burst size for the single rate two color mode. The unit is in kilobyte. *Rate Exceeded* – Specify the action for packets that exceed the committed rate in single rate two color mode. The action can be specified as one of the following: *Drop Packet* – Drop the packet immediately. *Remark DSCP* – Mark the packet with a specified DSCP. The packet is set to drop for packets with a high precedence. **trTCM** – Specify the “two-rate three-color mode.” *CIR* – Specify the Committed information Rate. The unit is Kbps. CIR should always be equal or less than PIR. *PIR* – Specify the Peak information Rate. The unit is Kbps. PIR should always be equal to or greater than CIR. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *PBS* – Specify the Peak Burst Size. The unit is in kilobyte. **srTCM** – Specify the “single-rate three-color mode”. *CIR* – Specify the Committed Information Rate. The unit is in kilobyte. *CBS* – Specify the Committed Burst Size. The unit is in kilobyte. *EBS* – Specify the Excess Burst Size. The unit is in kilobyte.
Action	**Conform** – This field denotes the green packet flow. Green packet flows may have their *DSCP* field rewritten to a value stated in this field. Users may also choose to count green packets by using counter parameter.

	Replace DSCP – Packets that are in the green flow may have their DSCP field rewritten using this parameter and entering the DSCP value to replace. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the green flow. **Exceed** – This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the yellow flow. **Violate** – This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. *Counter* – Use this parameter to enable or disable the packet counter for the specified ACL entry in the red flow.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Apply** button to accept the changes made.

After clicking the **View** button, the following page will appear:



Profile ID	1			
Access ID	1			
Mode	Rate	Rate (Kbps)		200
		Burst Size (Kbyte)		200
		Rate Exceeded	Remark DSCP	1

Figure 7-66 Egress ACL Flow meter Display window

Click the **<<Back** button to return to the previous page.

Chapter 8 Security

802.1X
RADIUS
IP-MAC-Port Binding (IMPB) (EI Mode Only)
MAC-based Access Control (MAC)
Web-based Access Control (WAC)
Japanese Web-based Access Control (JWAC)
Compound Authentication
IGMP Access Control Settings
Port Security
ARP Spoofing Prevention Settings
BPDU Attack Protection
Loopback Detection Settings
RPC PortMapper Filter Settings
NetBIOS Filtering Settings
Traffic Segmentation Settings
DHCP Server Screening
Access Authentication Control
SSL Settings
SSH
Trusted Host Settings
Safeguard Engine Settings

802.1X

802.1X (Port-Based and Host-Based Access Control)

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

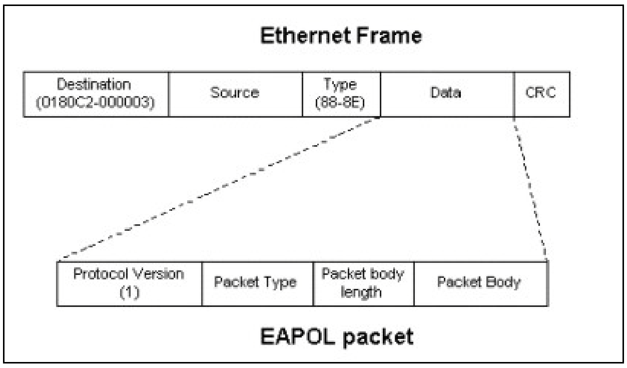

Ethernet Frame
Destination (0180C2-000003)
Source
Type (88-8E)
Data
CRC
Protocol Version (1)
Packet Type
Packet body length
Packet Body
EAPOL packet

Figure 8-1 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1X Access Control method has three roles, each of which are vital to creating and up keeping a stable and working Access Control security method.

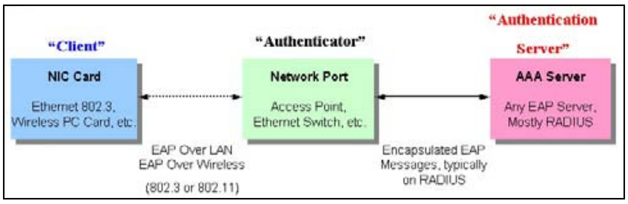

"Client"
NIC Card
Ethernet 802.3, Wireless PC Card, etc.
"Authenticator"
Network Port
Access Point, Ethernet Switch, etc.
"Authentication Server"
AAA Server
Any EAP Server, Mostly RADIUS
EAP Over LAN
EAP Over Wireless
(802.3 or 802.11)
Encapsulated EAP Messages, typically on RADIUS

Figure 8-2 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

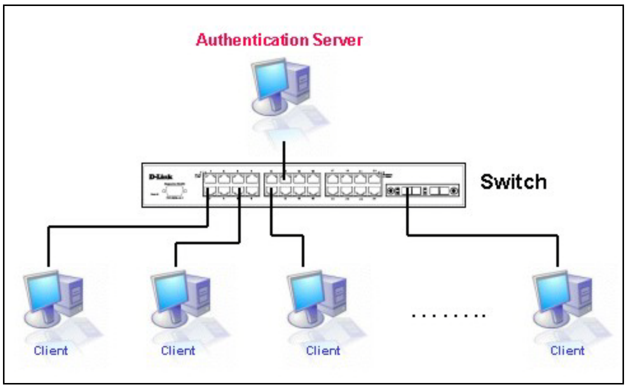


Figure 8-3 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing the 802.1X function. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

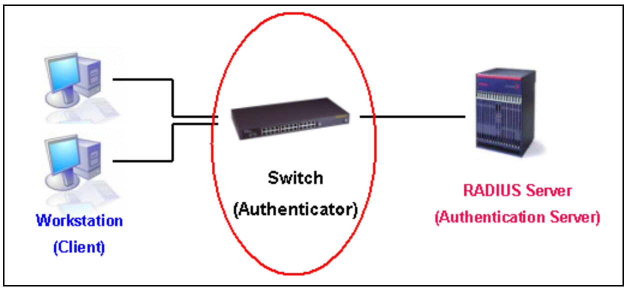


Figure 8-4 The Authenticator

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X State must be *Enabled*. (**Security / 802.1X /802.1X Settings**)
2. The 802.1X settings must be implemented by port (**Security** / **802.1X** / **802.1X Settings**)
3. A RADIUS server must be configured on the Switch. (**Security** / **802.1X** / **Authentic RADIUS Server**)

Client

The Client is simply the end station that wishes to gain access to the LAN or switch services. All end stations must be running software that is compliant with the 802.1X protocol. For users running Windows XP and Windows Vista, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

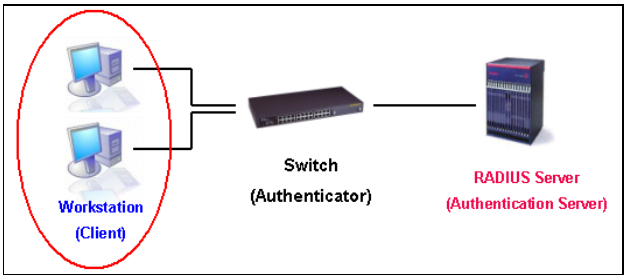


Figure 8-5 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is "locked" until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully "unlocks" the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

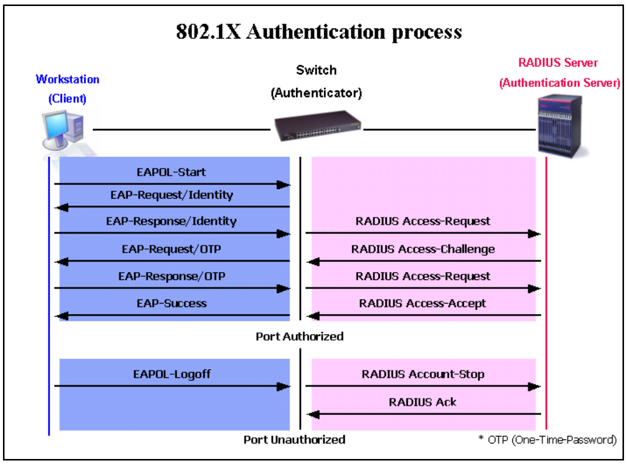

802.1X Authentication process
Workstation
(Client)
Switch
(Authenticator)
RADIUS Server
(Authentication Server)
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request/OTP
EAP-Response/OTP
EAP-Success
RADIUS Access-Request
RADIUS Access-Challenge
RADIUS Access-Request
RADIUS Access-Accept
Port Authorized
EAPOL-Logoff
RADIUS Account-Stop
RADIUS Ack
Port Unauthorized
* OTP (One-Time-Password)

Figure 8-6 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. Host-Based Access Control – Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and Host-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

Port-Based Network Access Control

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

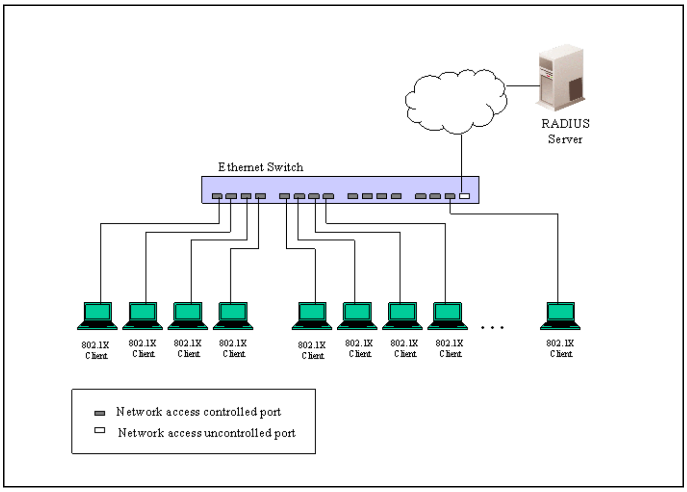

RADIUS Server
Ethernet Switch
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
. . .
802.1X Client
Network access controlled port
Network access uncontrolled port

Figure 8-7 Example of Typical Port-based Configuration

Host-Based Network Access Control

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

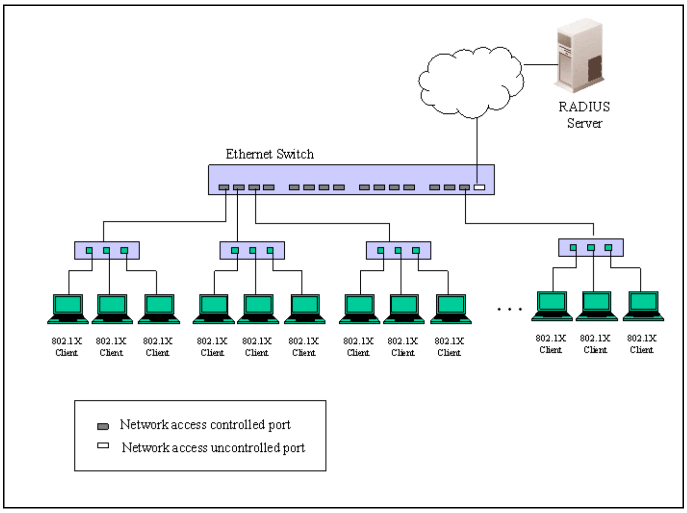
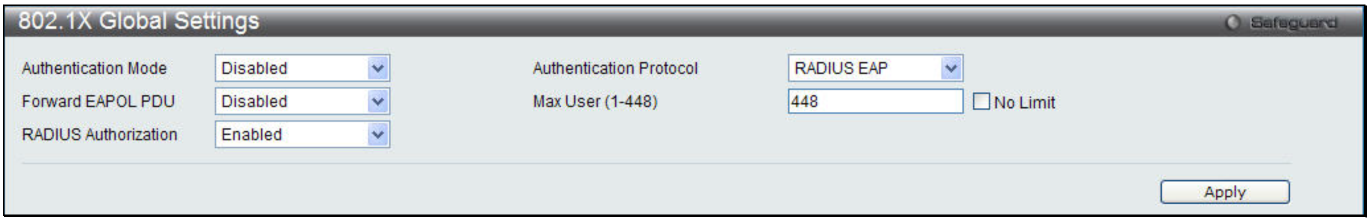

RADIUS Server
Ethernet Switch
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
802.1X Client
▬ Network access controlled port
▭ Network access uncontrolled port

Figure 8-8 Example of Typical Host-based Configuration

802.1X Global Settings

Users can configure the 802.1X global parameter.

To view this window, click **Security > 802.1X > 802.1X Global Settings** as shown below:


802.1X Global Settings
Safeguard
Apply

Authentication Mode: Disabled
Forward EAPOL PDU: Disabled
RADIUS Authorization: Enabled
Authentication Protocol: RADIUS EAP
Max User (1-448): 448 ☐ No Limit

Figure 8-9 802.1X Global Settings window

The fields that can be configured are described below:

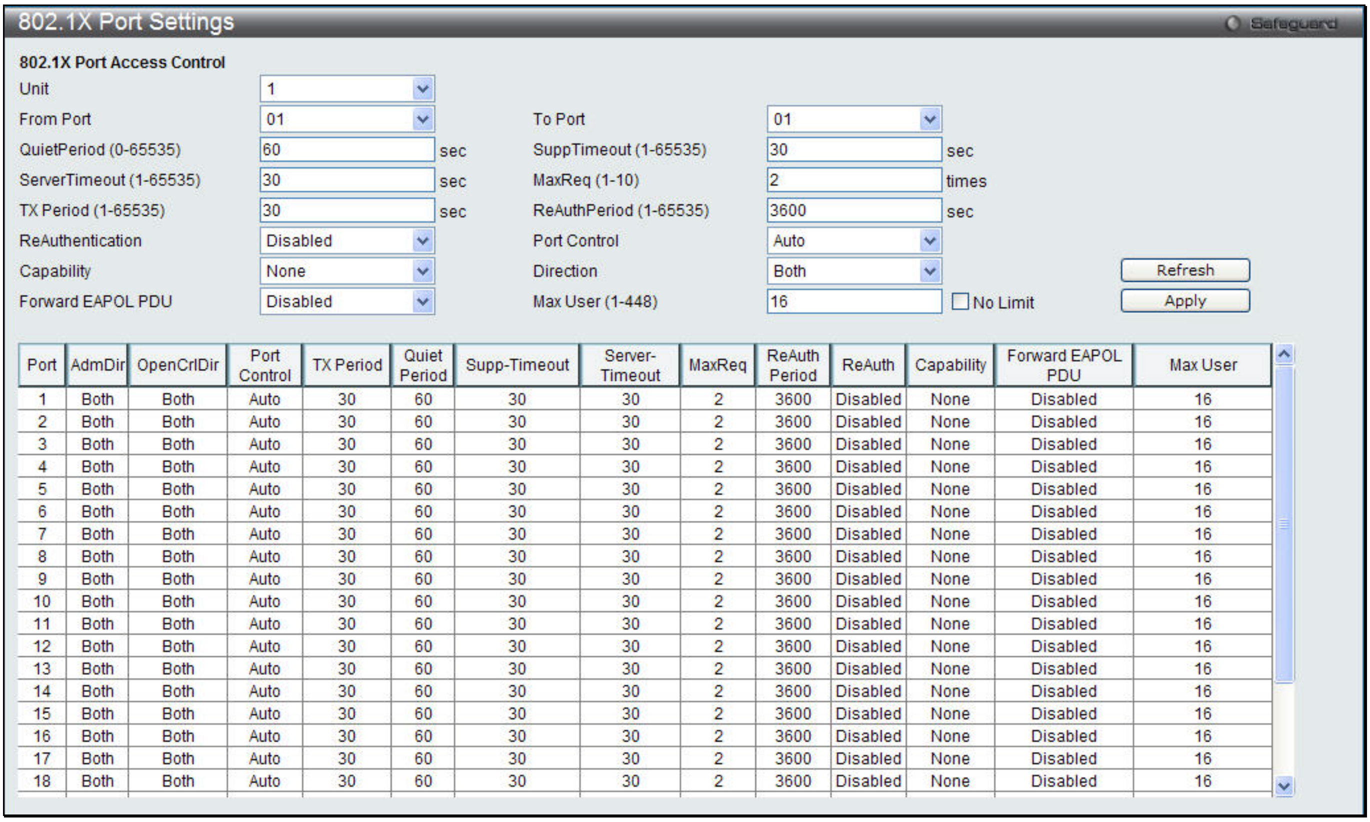
Parameter	Description
Authentication Mode	Choose the 802.1X authenticator mode, *Disabled*, *Port-based*, or *MAC-based*.
Authentication Protocol	Choose the authenticator protocol, *Local* or *RADIUS EAP*.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max Users (1-448)	Specifies the maximum number of users. The limit on the maximum users is *448* users. Tick the **No Limit** check box to have unlimited users.
RADIUS Authorization	This option is used to enable or disable acceptation of authorized configuration. When the authorization is enabled for 802.1X’s RADIUS, the authorized data assigned by the RADIUS server will be accepted if the global authorization network is enabled.

Click the **Apply** button to accept the changes made.

802.1X Port Settings

Users can configure the 802.1X authenticator port settings.

To view this window, click **Security > 802.1X > 802.1X Port Settings** as shown below:



802.1X Port Access Control

Unit	1		
From Port	01	To Port	01
QuietPeriod (0-65535)	60 sec	SuppTimeout (1-65535)	30 sec
ServerTimeout (1-65535)	30 sec	MaxReq (1-10)	2 times
TX Period (1-65535)	30 sec	ReAuthPeriod (1-65535)	3600 sec
ReAuthentication	Disabled	Port Control	Auto
Capability	None	Direction	Both
Forward EAPOL PDU	Disabled	Max User (1-448)	16 ☐ No Limit

Port	AdmDir	OpenCrlDir	Port Control	TX Period	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Forward EAPOL PDU	Max User
1	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
2	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
3	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
4	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
5	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
6	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
7	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
8	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
9	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
10	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
11	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
12	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
13	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
14	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
15	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
16	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
17	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16
18	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Disabled	16

Figure 8-10 802.1X Port Settings

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports you wish to configure.
QuietPeriod (0-65535)	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is *60* seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is *30* seconds. It is defined in SuppTimeout, IEEE-802.1X-2001, page 47. The initialization value is used for the awhile timer when timing out the Supplicant. Its default value is 30 seconds; however, if the type of challenge involved in the current exchange demands a different value of timeout (for example, if the challenge requires an action on the part of the user), then the timeout value is adjusted accordingly. It can be set by management to any value in the range from 1 to 65535 seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is *30* seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is *2*. It is defined in MaxReq, IEEE-802.1X-2001 page 47. The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. Its default value is 2; it can be set by management to any value in the range from 1 to 10.

TxPeriod (1-65535)	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is *30* seconds.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic re-authentication of the client. The default setting is *3600* seconds.
ReAuthentication	Determines whether regular re-authentication will take place on this port. The default setting is *Disabled*.
Port Control	This allows the user to control the port authorization state. Select *ForceAuthorized* to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If *ForceUnauthorized* is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If *Auto* is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is *Auto*.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select *Authenticator* to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select *None* disable 802.1X functions on the port.
Direction	Sets the administrative-controlled direction to *Both* or *In.* If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. If *In* is selected, the control is only exerted over incoming traffic through the port the user selected in the first field.
Forward EAPOL PDU	This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.
Max Users (1-448)	Specifies the maximum number of users. The maximum user limit is 448 users. The default is 16. Tick the **No Limit** check box to have unlimited users.

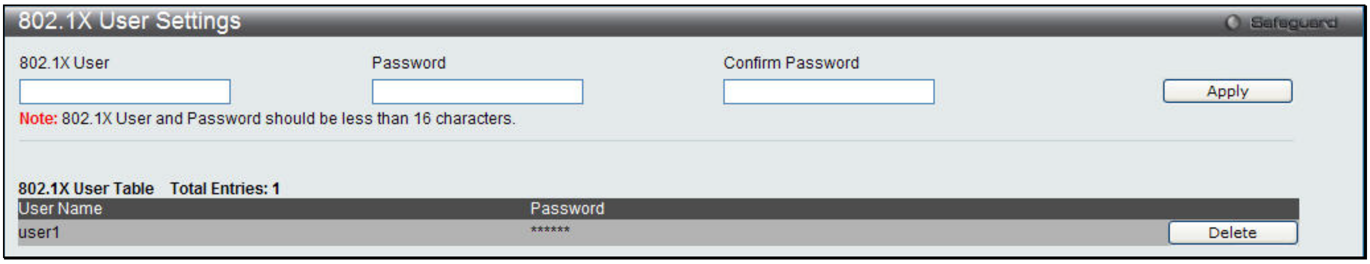
Click the **Refresh** button to refresh the display table so that new entries will appear.

Click the **Apply** button to accept the changes made.

802.1X User Settings

Users can set different 802.1X users in switch’s local database.

To view this window, click **Security > 802.1X > 802.1X User Settings** as shown below:


802.1X User Settings

802.1X User | Password | Confirm Password

Note: 802.1X User and Password should be less than 16 characters.

802.1X User Table Total Entries: 1

User Name	Password	
user1	******	Delete

Safeguard
Apply

Figure 8-11 802.1X User Settings window

The fields that can be configured are described below:

Parameter	Description
802.1X User	The user can enter an 802.1X user's username in here.
Password	The user can enter an 802.1X user's password in here.
Confirm Password	The user can re-enter an 802.1X user's password in here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

NOTE: The **802.1X User** and **Password** values should be less than 16 characters.

Guest VLAN Settings

On 802.1X security-enabled networks, there is a need for non- 802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or older operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement 802.1X Guest VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN.

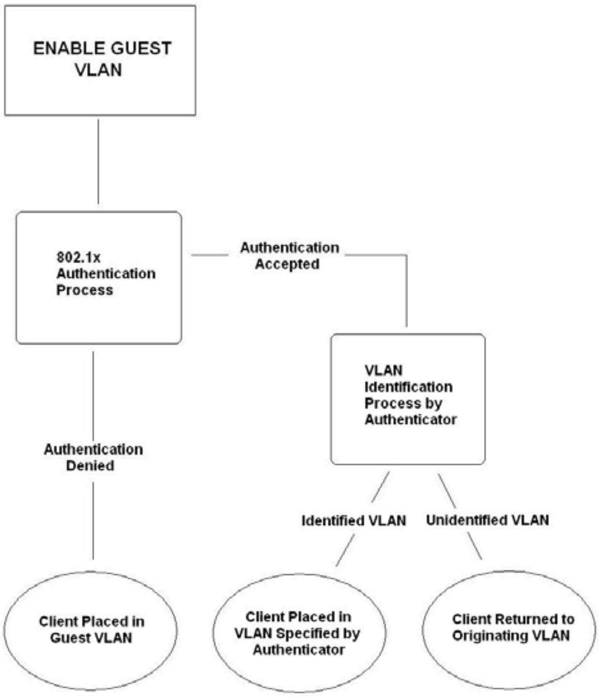

ENABLE GUEST VLAN
802.1x Authentication Process
Authentication Accepted
VLAN Identification Process by Authenticator
Authentication Denied
Identified VLAN
Unidentified VLAN
Client Placed in Guest VLAN
Client Placed in VLAN Specified by Authenticator
Client Returned to Originating VLAN

Figure 8-12 Guest VLAN Authentication Process

If authenticated and the authenticator possess the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

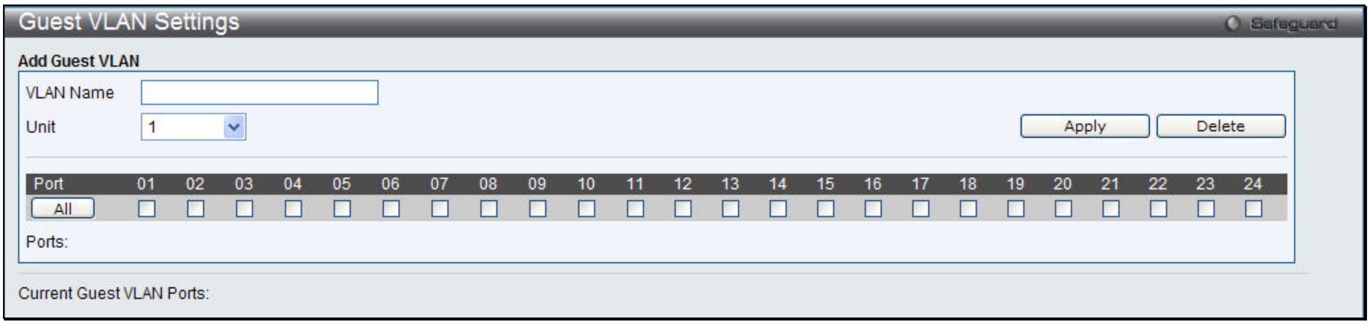
Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.

2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

Remember, to set an 802.1X guest VLAN, the user must first configure a normal VLAN, which can be enabled here for guest VLAN status. Only one VLAN may be assigned as the 802.1X guest VLAN.

To view this window, click **Security > 802.1X > Guest VLAN Settings** as shown below:


Guest VLAN Settings
Safeguard
Add Guest VLAN
VLAN Name
Apply
Delete
Port
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
All
Ports:
Current Guest VLAN Ports:

Unit: 1

Figure 8-13 Guest VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as an 802.1X guest VLAN.
Unit	Specify a unit to be configured.
Port	Set the ports to be enabled for the 802.1X guest VLAN. Click the **All** button to select all the ports.

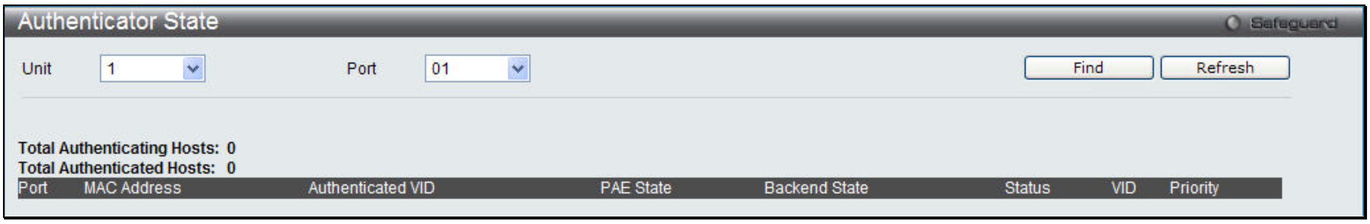
Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry based on the information entered.

Authenticator State

This window is used to display the authenticator state.

To view this window, click **Security > 802.1X > Authenticator State** as shown below:


Authenticator State
Safeguard
Find
Refresh
Port
MAC Address
Authenticated VID
PAE State
Backend State
Status
VID
Priority

Unit: 1

Port: 01

Total Authenticating Hosts: 0

Total Authenticated Hosts: 0

Figure 8-14 Authenticator State window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
Port	Select a port to be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

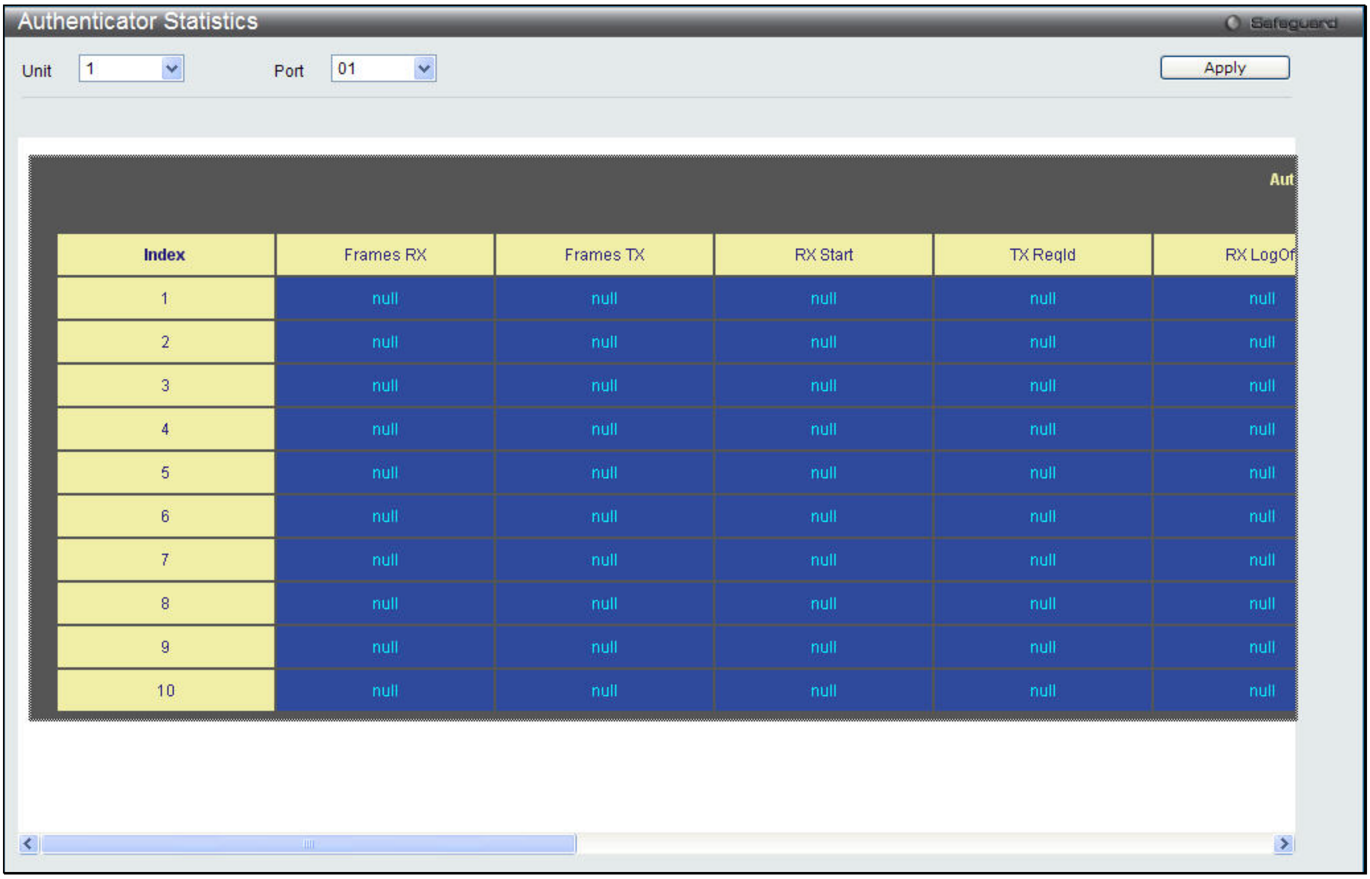
Click the **Refresh** button to refresh the display table so that new entries will appear.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Statistics

This window is used to display the authenticator statistics information.

To view this window, click **Security > 802.1X > Authenticator Statistics** as shown below:



Unit 1 Port 01

Index	Frames RX	Frames TX	RX Start	TX ReqId	RX LogOf
1	null	null	null	null	null
2	null	null	null	null	null
3	null	null	null	null	null
4	null	null	null	null	null
5	null	null	null	null	null
6	null	null	null	null	null
7	null	null	null	null	null
8	null	null	null	null	null
9	null	null	null	null	null
10	null	null	null	null	null

Figure 8-15 Authenticator Statistics window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
Port	Select a port to be displayed.

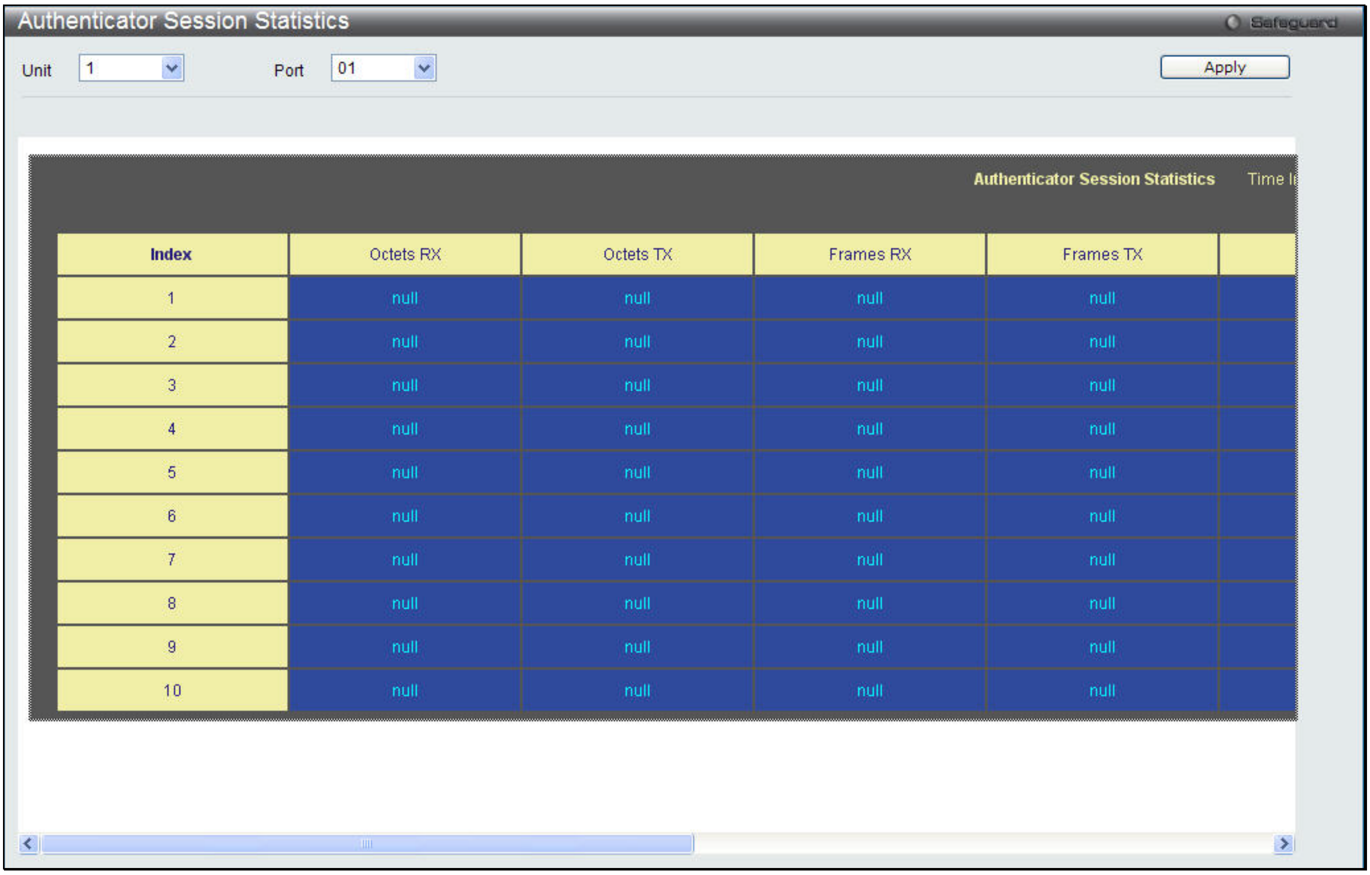
Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Session Statistics

This window is used to display the authenticator session statistics information.

To view this window, click **Security > 802.1X > Authenticator Session Statistics** as shown below:


Authenticator Session Statistics
Safeguard
Apply
Authenticator Session Statistics

Unit 1 Port 01

Index	Octets RX	Octets TX	Frames RX	Frames TX
1	null	null	null	null
2	null	null	null	null
3	null	null	null	null
4	null	null	null	null
5	null	null	null	null
6	null	null	null	null
7	null	null	null	null
8	null	null	null	null
9	null	null	null	null
10	null	null	null	null

Figure 8-16 Authenticator Session Statistics window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
Port	Select a port to be displayed.

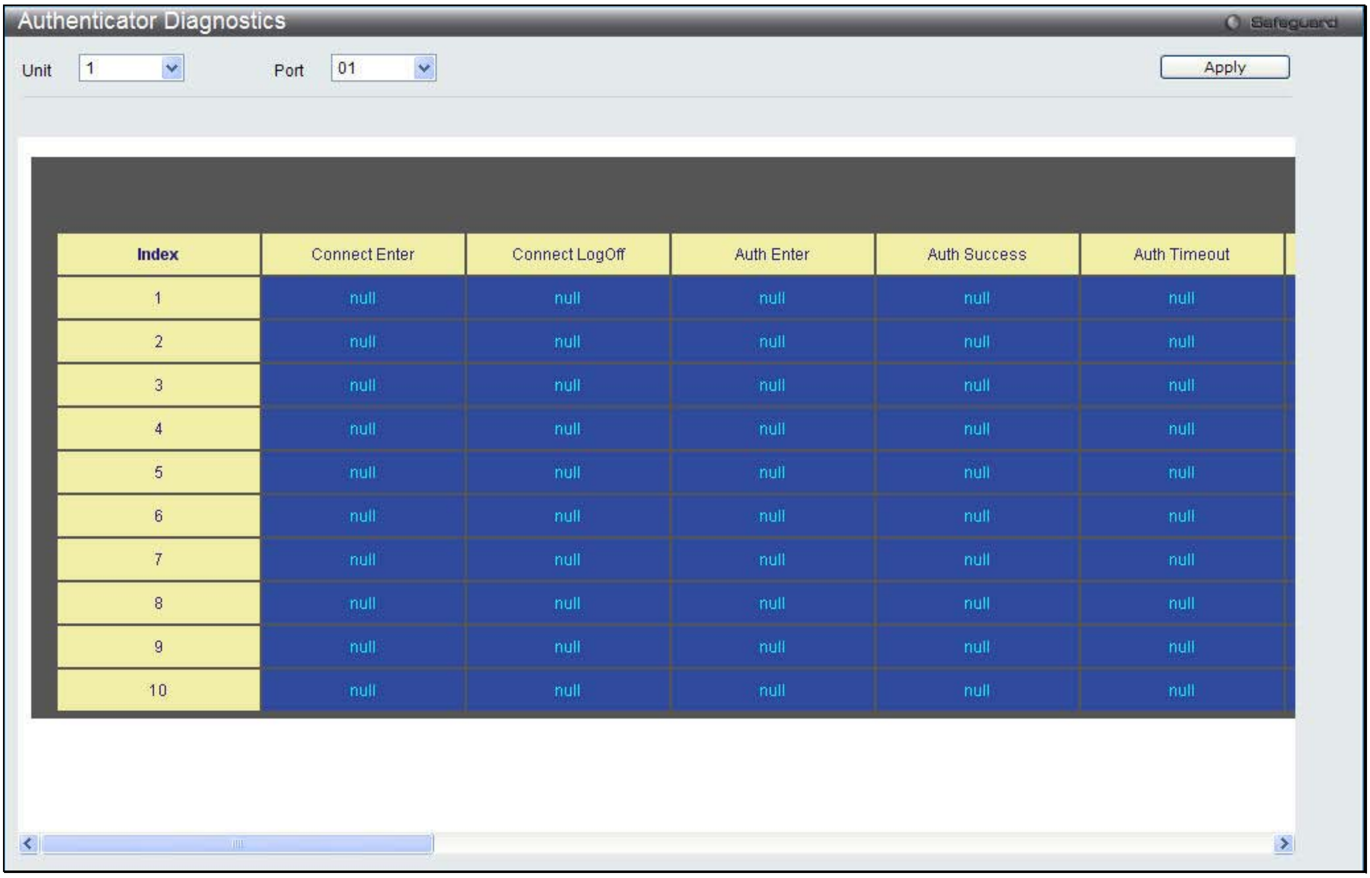
Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Authenticator Diagnostics

This window is used to display the authenticator diagnostics information.

To view this window, click **Security > 802.1X > Authenticator Diagnostics** as shown below:



Index	Connect Enter	Connect LogOff	Auth Enter	Auth Success	Auth Timeout
1	null	null	null	null	null
2	null	null	null	null	null
3	null	null	null	null	null
4	null	null	null	null	null
5	null	null	null	null	null
6	null	null	null	null	null
7	null	null	null	null	null
8	null	null	null	null	null
9	null	null	null	null	null
10	null	null	null	null	null

Figure 8-17 Authenticator Diagnostics window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
Port	Select a port to be displayed.

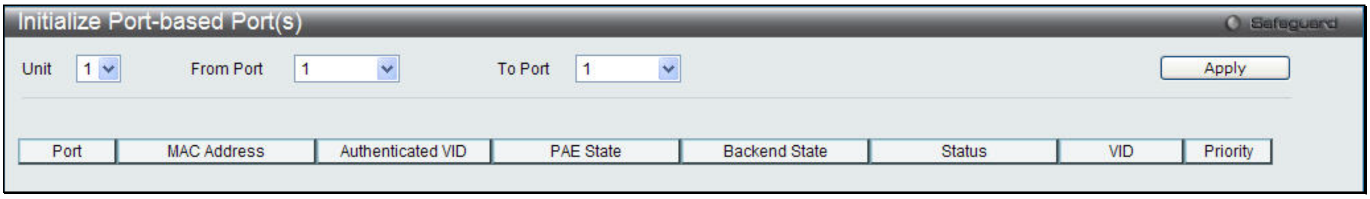
Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Initialize Port-based Port(s)

This window is used to display the authenticator diagnostics information.

To view this window, click **Security > 802.1X > Initialize Port-based Port(s)** as shown below:



Port	MAC Address	Authenticated VID	PAE State	Backend State	Status	VID	Priority

Figure 8-18 Initialize Port-based Port(s) window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
From Port / To Port	Select a range of ports to be displayed.

Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Initialize Host-based Port(s)

This window is used to display the current initialized host-based ports.

To view this window, click **Security > 802.1X > Initialize Host-based Port(s)** as shown below:

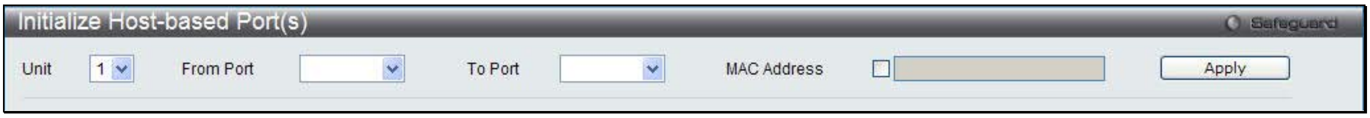

Initialize Host-based Port(s)
Safeguard
Unit
1
From Port
To Port
MAC Address
Apply

Figure 8-19 Initialize Host-based Port(s) window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
From Port / To Port	Select a range of ports to be displayed.
MAC Address	Tick the check box and enter the authenticated MAC address of the client connected to the corresponding port.

Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Reauthenticate Port-based Port(s)

This window is used to display the current status of the re-authenticated port-based port(s).

To view this window, click **Security > 802.1X > Reauthenticate Port-based Port(s)** as shown below:

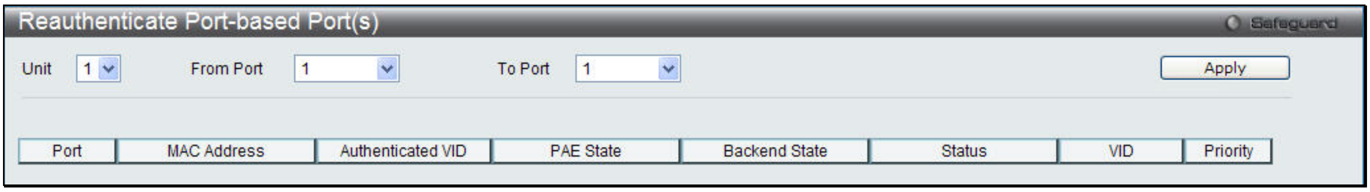

Reauthenticate Port-based Port(s)
Safeguard
Unit
1
From Port
1
To Port
1
Apply
Port
MAC Address
Authenticated VID
PAE State
Backend State
Status
VID
Priority

Figure 8-20 Reauthenticate Port-based Port(s) window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
From Port / To Port	Select a range of ports to be displayed.

Click the **Apply** button to accept the changes made.

NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

Reauthenticate Host-based Port(s)

This window is used to display the current status of the re-authenticated host-based port(s).

To view this window, click **Security > 802.1X > Reauthenticate Host-based Port(s)** as shown below:

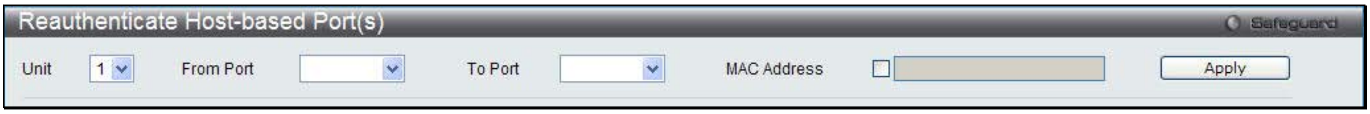

Reauthenticate Host-based Port(s)
Safeguard
Unit
1
From Port
To Port
MAC Address
☐
Apply

Figure 8-21 Reauthentiate Host-based Port(s) window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit to be displayed.
From Port / To Port	Select a range of ports to be displayed.
MAC Address	Tick the check box and enter the authenticated MAC address of the client connected to the corresponding port.

Click the **Apply** button to accept the changes made.

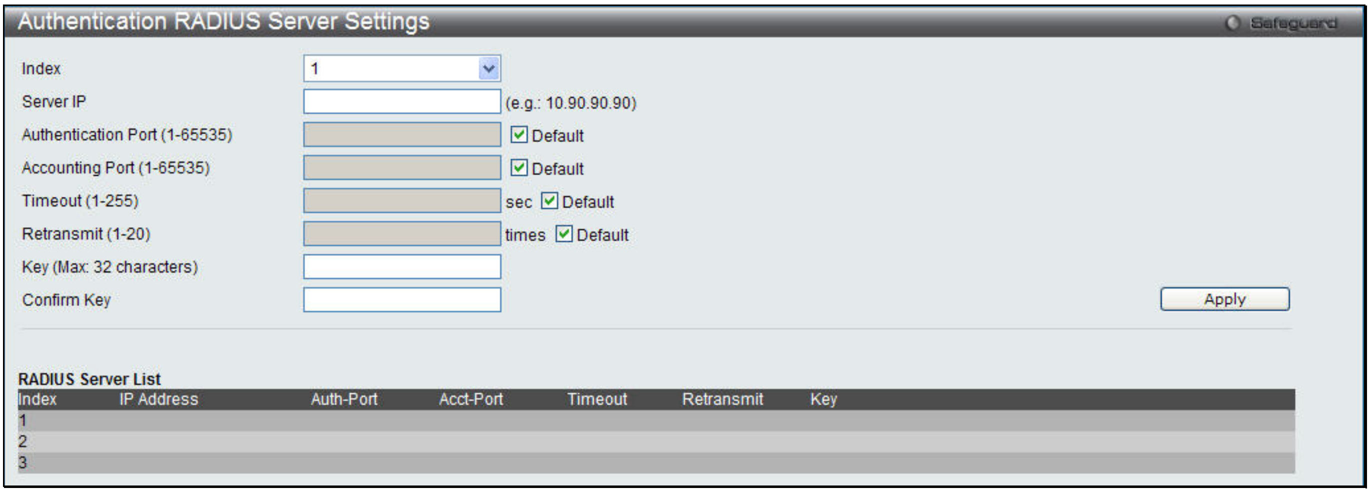
NOTE: The user must first globally enable **Authentication Mode** in the 802.1X Global Settings window before initializing ports. Information in this window cannot be viewed before enabling the authentication mode for either **Port-based** or **MAC-based**.

RADIUS

Authentication RADIUS Server Settings

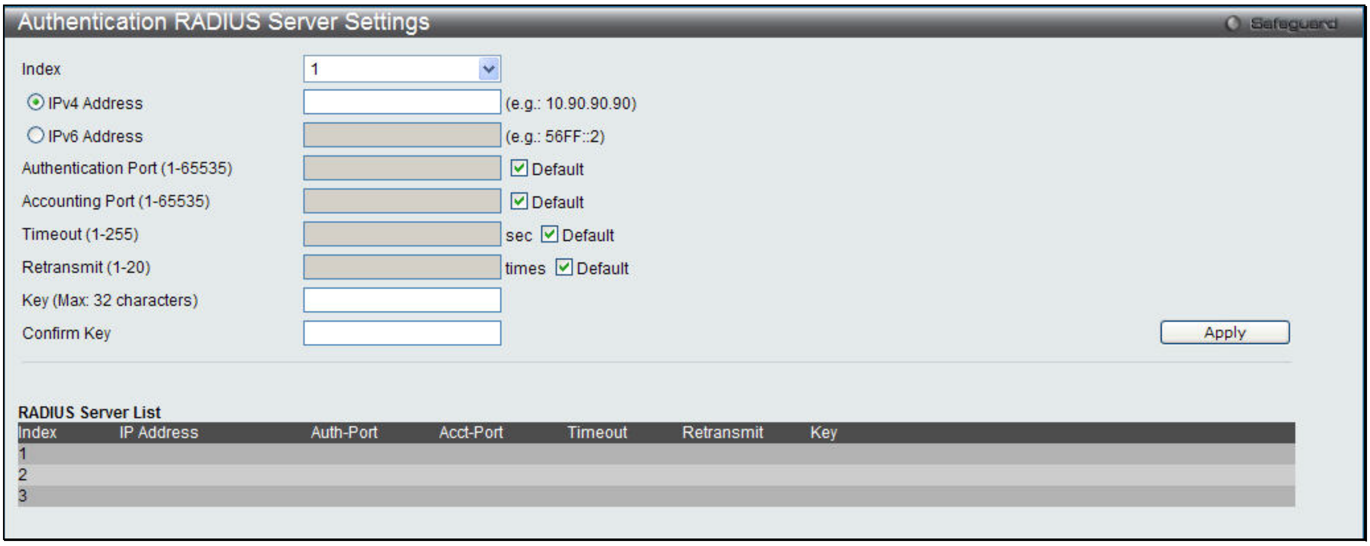
The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

To view this window, click **Security > RADIUS > Authentication RADIUS Server Settings** as shown below:


Authentication RADIUS Server Settings
Safeguard
Index
1
Server IP
(e.g.: 10.90.90.90)
Authentication Port (1-65535)
☑ Default
Accounting Port (1-65535)
☑ Default
Timeout (1-255)
sec ☑ Default
Retransmit (1-20)
times ☑ Default
Key (Max: 32 characters)
Confirm Key
Apply
RADIUS Server List

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1						
2						
3						

Figure 8-22 Authentication RADIUS Server Settings window (SI Mode Only)



Index	1
● IPv4 Address	(e.g.: 10.90.90.90)
○ IPv6 Address	(e.g.: 56FF::2)
Authentication Port (1-65535)	☑ Default
Accounting Port (1-65535)	☑ Default
Timeout (1-255)	sec ☑ Default
Retransmit (1-20)	times ☑ Default
Key (Max: 32 characters)	
Confirm Key	

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1						
2						
3						

Figure 8-23 Authentication RADIUS Server Settings window (EI Mode Only)

The fields that can be configured are described below:

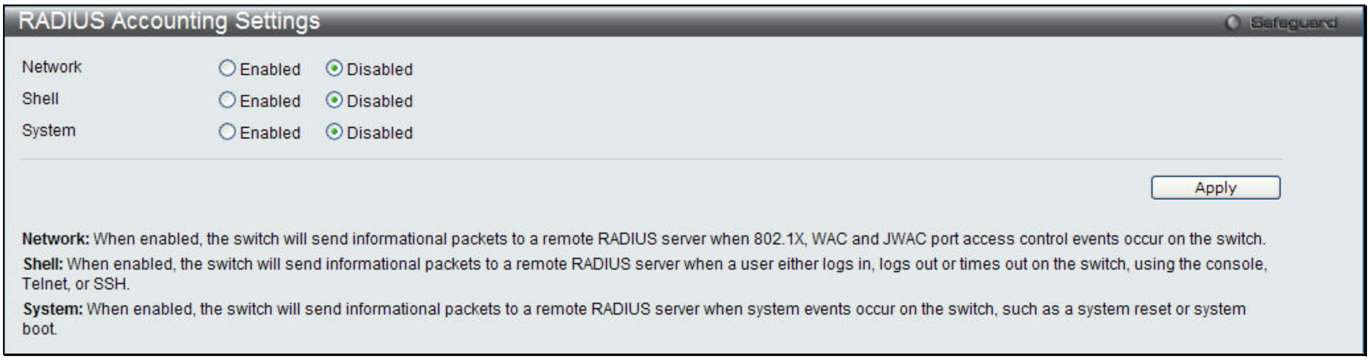
Parameter	Description
Index	Choose the desired RADIUS server to configure: *1, 2* or *3* and select the IPv4 Address.
Server IP (SI Mode Only)	Set the RADIUS server IP address.
IPv4 Address (EI Mode Only)	Set the RADIUS server IP address.
IPv6 Address (EI Mode Only)	Set the RADIUS server IPv6 address.
Authentication Port (1-65535)	Set the RADIUS authentic server(s) UDP port which is used to transmit RADIUS data between the Switch and the RADIUS server. The default port is *1812*.
Accounting Port (1-65535)	Set the RADIUS account server(s) UDP port which is used to transmit RADIUS accounting statistics between the Switch and the RADIUS server. The default port is *1813*.
Timeout (1-255)	Set the RADIUS server age-out, in seconds.
Retransmit (1-20)	Set the RADIUS server retransmit time, in times.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the key the same as that of the RADIUS server.

Click the **Apply** button to accept the changes made.

RADIUS Accounting Settings

Users can configure the state of the specified RADIUS accounting service.

To view this window, click **Security > RADIUS > RADIUS Accounting Settings** as shown below:



Network ○ Enabled ● Disabled
Shell ○ Enabled ● Disabled
System ○ Enabled ● Disabled

Network: When enabled, the switch will send informational packets to a remote RADIUS server when 802.1X, WAC and JWAC port access control events occur on the switch.

Shell: When enabled, the switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the switch, using the console, Telnet, or SSH.

System: When enabled, the switch will send informational packets to a remote RADIUS server when system events occur on the switch, such as a system reset or system boot.

Figure 8-24 RADIUS Accounting Settings window

The fields that can be configured are described below:

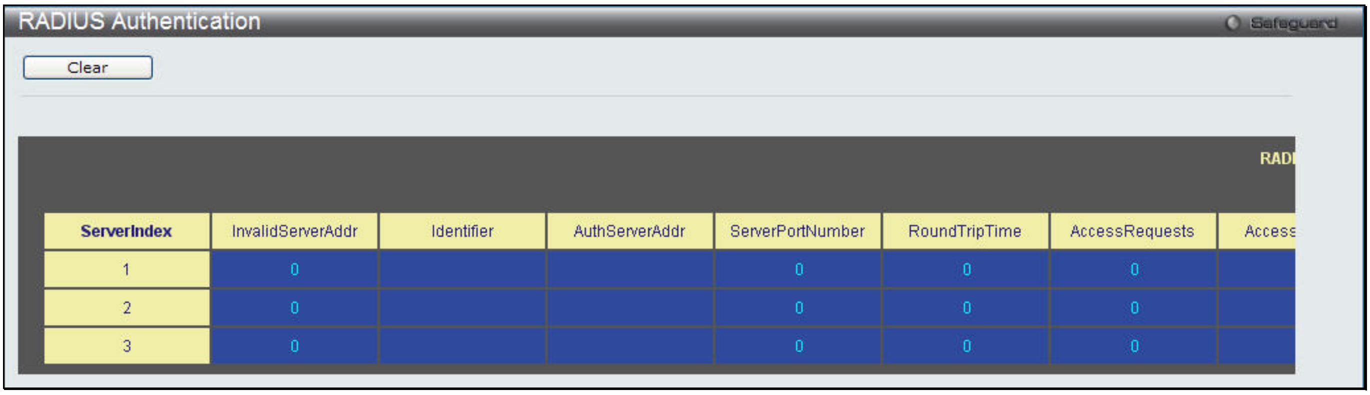
Parameter	Description
Network	When enabled, the Switch will send informational packets to a remote RADIUS server when 802.1X and WAC port access control events occur on the Switch.
Shell	When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.
System	When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

Click the **Apply** button to accept the changes made.

RADIUS Authentication

Users can display information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view this window, click **Security > RADIUS > RADIUS Authentication** as shown below:



ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	Access
1	0			0	0	0	
2	0			0	0	0	
3	0			0	0	0	

Figure 8-25 RAIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The fields that can be configured are described below:

Parameter	Description
InvalidServerAddr	The number of RADIUS Access-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS authentication client.
ServerIndex	The identification number assigned to each RADIUS Authentication server that the

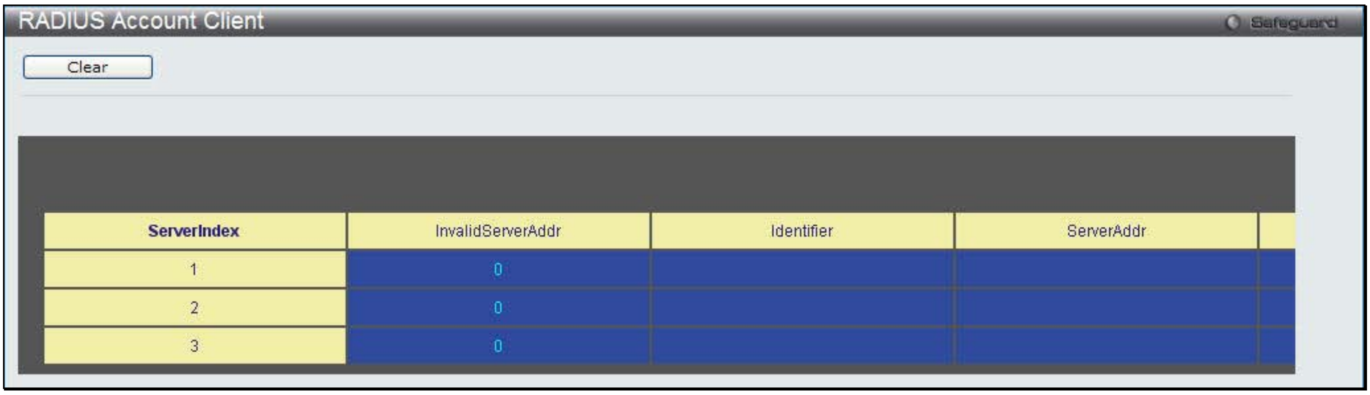
	client shares a secret with.
AuthServerAddr	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
AccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
AccessRetrans	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
AccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
AccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
AccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
AccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
BadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
PendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
Timeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
PacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Click the **Clear** button to clear the current statistics shown.

RADIUS Account Client

Users can display managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view this window, click **Security > RADIUS > RADIUS Account Client** as shown below:



ServerIndex	InvalidServerAddr	Identifier	ServerAddr
1	0		
2	0		
3	0		

Figure 8-26 RADIUS Account Client window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The fields that can be configured are described below:

Parameter	Description
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
InvalidServerAddr	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client.
ServerAddr	The IP address of the RADIUS authentication server referred to in this table entry.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

Click the **Clear** button to clear the current statistics shown.

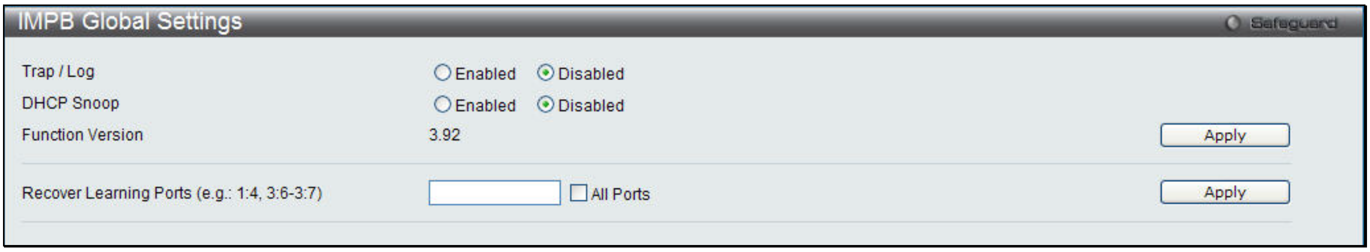
IP-MAC-Port Binding (IMPB) (EI Mode Only)

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict the access to a switch to a number of authorized users. Authorized clients can access a switch's port by either checking the pair of IP-MAC addresses with the pre-configured database or if DHCP snooping has been enabled in which case the switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the IMPB white list. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. For the xStack® DGS-3120 series of switches, active and inactive entries use the same database. The maximum number of entries is 510. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

IMPB Global Settings

Users can enable or disable the Trap/Log State and DHCP Snoop state on the Switch. The Trap/Log field will enable and disable the sending of trap/log messages for IP-MAC-port binding. When enabled, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Global Settings** as shown below:



Trap / Log ○ Enabled ● Disabled

DHCP Snoop ○ Enabled ● Disabled

Function Version 3.92

Recover Learning Ports (e.g.: 1:4, 3:6-3:7) ☐ All Ports

Figure 8-27 IMPB Global Settings

The fields that can be configured are described below:

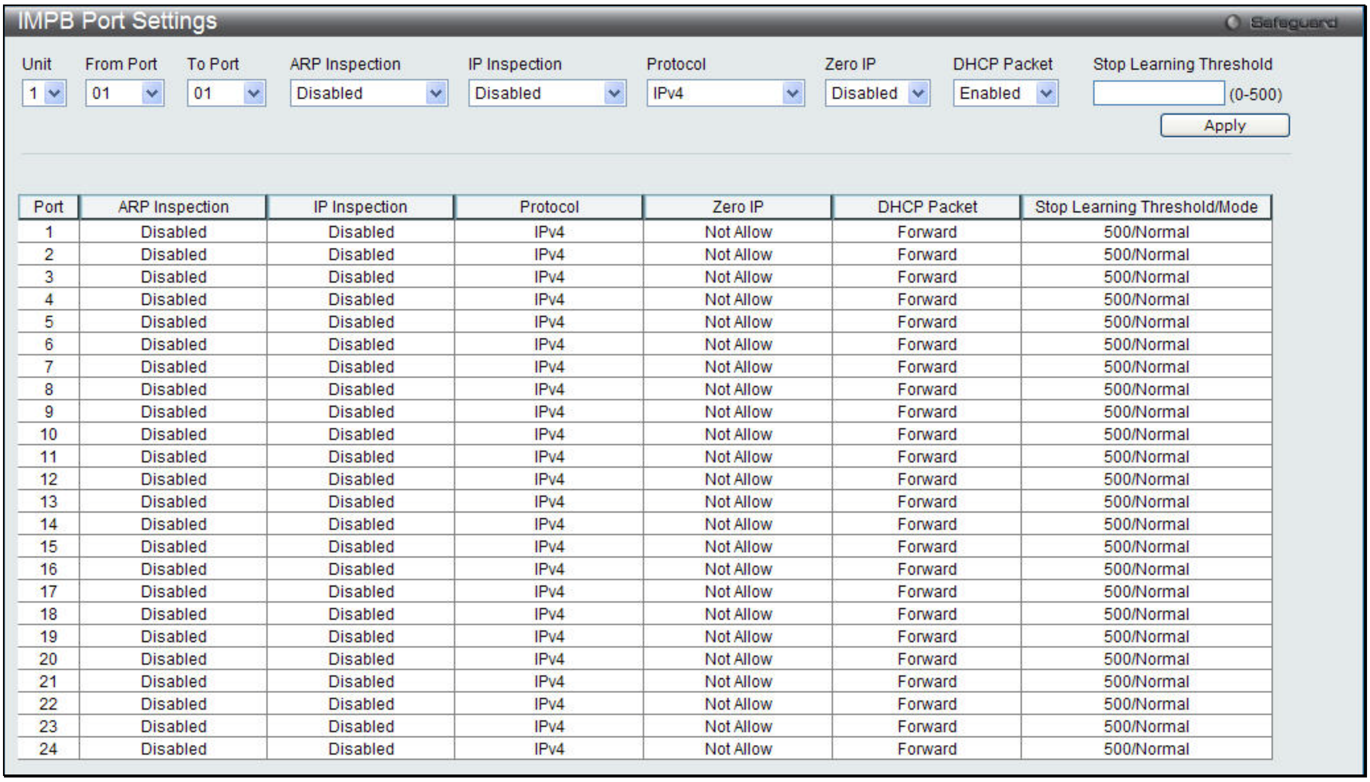
Parameter	Description
Trap / Log	Click the radio buttons to enable or disable the sending of trap/log messages for IP-MAC-port binding. When *Enabled*, the Switch will send a trap message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC-port binding configuration set on the Switch. The default is *Disabled*.
DHCP Snooping	Click the radio buttons to enable or disable DHCP snooping for IP-MAC-port binding. The default is *Disabled*.
Recover Learning Ports	Enter the port numbers used to recover the learning port state. Tick the **All** check box to apply to all ports.

Click the **Apply** button to accept the changes made for each individual section.

IMPB Port Settings

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with the State, Allow Zero IP and Forward DHCP Packet field, and configure the port's Max Entry.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Port Settings** as shown below:



Unit	From Port	To Port	ARP Inspection	IP Inspection	Protocol	Zero IP	DHCP Packet	Stop Learning Threshold
1	01	01	Disabled	Disabled	IPv4	Disabled	Enabled	(0-500)

Port	ARP Inspection	IP Inspection	Protocol	Zero IP	DHCP Packet	Stop Learning Threshold/Mode
1	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
2	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
3	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
4	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
5	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
6	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
7	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
8	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
9	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
10	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
11	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
12	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
13	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
14	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
15	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
16	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
17	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
18	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
19	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
20	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
21	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
22	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
23	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal
24	Disabled	Disabled	IPv4	Not Allow	Forward	500/Normal

Figure 8-28 IMPB Port Settings window

The fields that can be configured are described below:

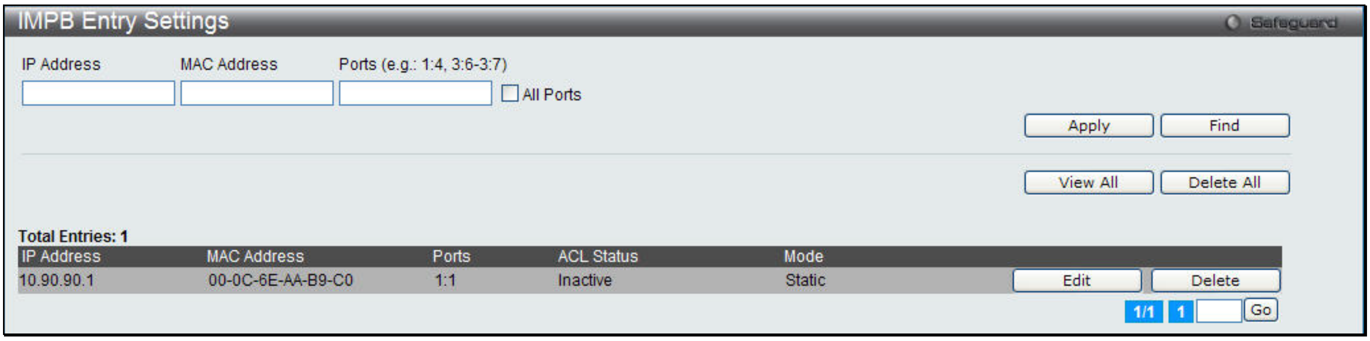
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports to set for IP-MAC-port binding.
ARP Inspection	When the ARP inspection function is enabled, the legal ARP packets are forwarded, while the illegal packets are dropped. *Disabled* - Disable the ARP inspection function. *Enabled (Strict)* - This mode disables hardware learning of the MAC address. All packets are dropped by default until a legal ARP or IP packets are detected. When enabling this mode, the Switch stops writing dropped FDB entries on these ports. If detecting legal packets, the Switch needs to write forward FDB entry. *Enabled (Loose)* - In this mode, all packets are forwarded by default until an illegal ARP packet is detected. The default value is Disabled.
IP Inspection	When both ARP and IP inspections are enabled, all IP packets are checked. The legal IP packets are forwarded, while the illegal IP packets are dropped. When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets (Ex. L2 packets, or ARP) are forwarded by default. The default value is Disabled.
Protocol	Use the drop-down menu to select the protocol.
Zero IP	Use the drop-down menu to enable or disable this feature. Allow zero IP configures the state which allows ARP packets with 0.0.0.0 source IP to bypass.
DHCP Packet	By default, the DHCP packet with broadcast DA will be flooded. When set to disable, the broadcast DHCP packet received by the specified port will not be forwarded in strict mode. This setting is effective when DHCP snooping is enabled, in the case when a DHCP packet which has been trapped by the CPU needs to be forwarded by the software. This setting controls the forwarding behavior in this situation.
Stop Learning Threshold	Here is displayed the number of blocked entries on the port. The default value is *500*.

Click the **Apply** button to accept the changes made.

IMPB Entry Settings

This window is used to create static IP-MAC-binding port entries and view all IMPB entries on the Switch.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > IMPB Entry Settings** as shown below:


IMPB Entry Settings
Safeguard
IP Address
MAC Address
Ports (e.g.: 1:4, 3:6-3:7)
☐ All Ports
Apply
Find
View All
Delete All
Edit
Delete
1/1
1
Go

Total Entries: 1

IP Address	MAC Address	Ports	ACL Status	Mode
10.90.90.1	00-0C-6E-AA-B9-C0	1:1	Inactive	Static

Figure 8-29 IMPB Entry Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	Enter the IP address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Tick the **All Ports** check box to configure this entry for all ports on the Switch.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Edit** button to configure the specified entry.

Click the **Delete** button to remove the specified entry.

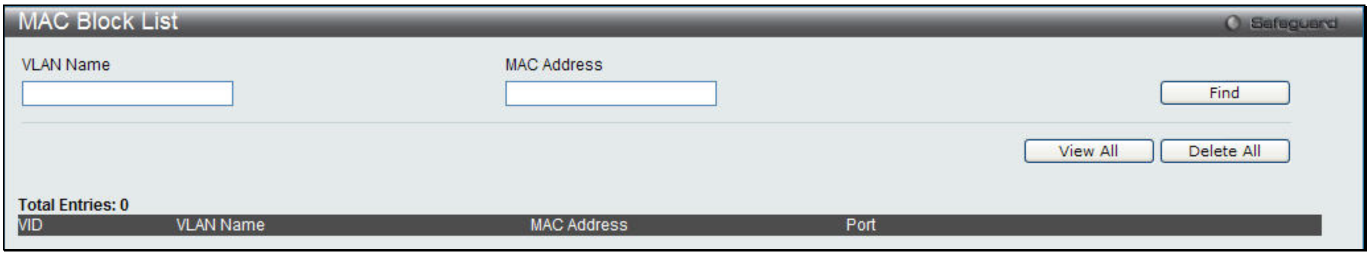
Click the **View All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

MAC Block List

This window is used to view unauthorized devices that have been blocked by IP-MAC binding restrictions.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > MAC Block List** as shown below:


MAC Block List
Safeguard
VLAN Name
MAC Address
Find
View All
Delete All

Total Entries: 0

VID	VLAN Name	MAC Address	Port

Figure 8-30 MAC Block List

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Enter a VLAN Name.
MAC Address	Enter a MAC address.

Click the **Find** button to find an unauthorized device that has been blocked by the IP-MAC binding restrictions

Click the **View All** button to display all the existing entries.

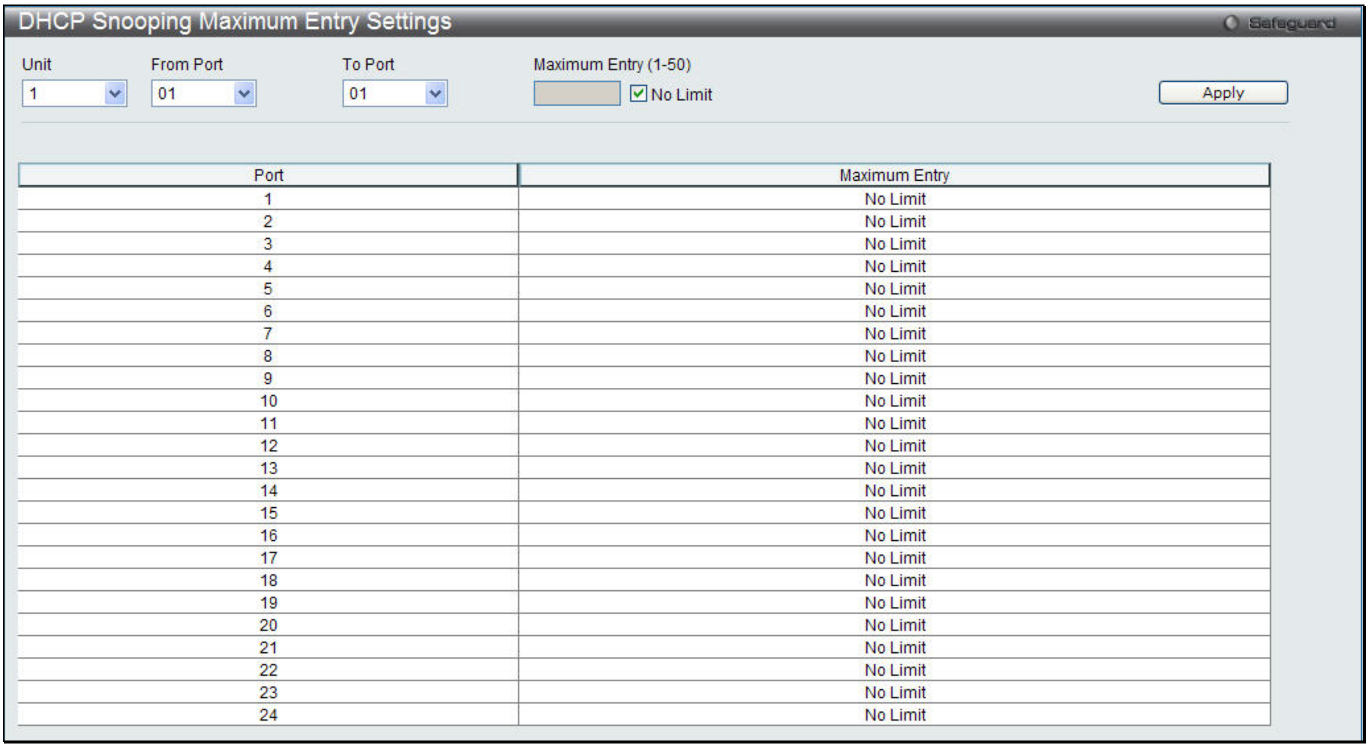
Click the **Delete All** button to remove all the entries listed.

DHCP Snooping

DHCP Snooping Maximum Entry Settings

Users can configure the maximum DHCP snooping entry for ports on this page.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entry Settings** as shown below:



Unit: 1

From Port: 01

To Port: 01

Maximum Entry (1-50): ☑ No Limit

Port	Maximum Entry
1	No Limit
2	No Limit
3	No Limit
4	No Limit
5	No Limit
6	No Limit
7	No Limit
8	No Limit
9	No Limit
10	No Limit
11	No Limit
12	No Limit
13	No Limit
14	No Limit
15	No Limit
16	No Limit
17	No Limit
18	No Limit
19	No Limit
20	No Limit
21	No Limit
22	No Limit
23	No Limit
24	No Limit

Figure 8-31 DHCP Snooping Max Entry Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to use.
Maximum Entry (1-50)	Enter the maximum entry value. Tick the **No Limit** check box to lift the maximum entry.

Click the **Apply** button to accept the changes made.

DHCP Snooping Entry

This window is used to view dynamic entries on specific ports.

To view this window, click **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry** as shown below:

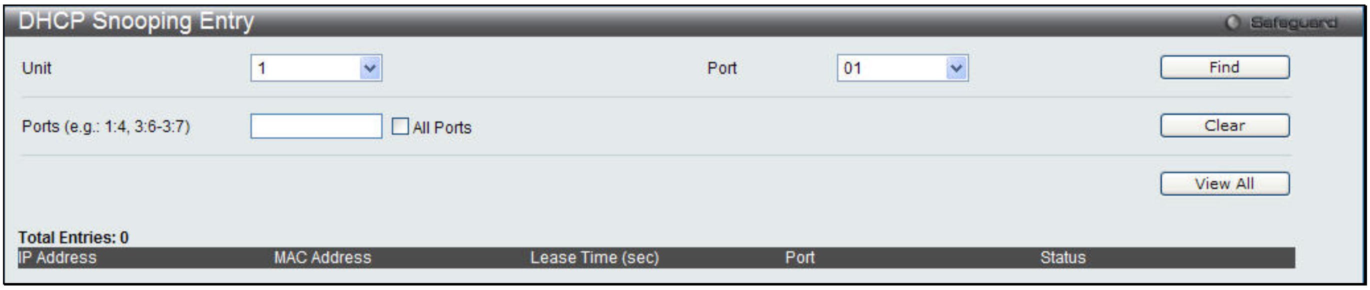


Figure 8-32 DHCP Snooping Entry window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to select the desired port.
Ports	Specify the ports for which to view DHCP snooping entries. Tick the **All Ports** check box to clear entries for all ports.

Click the **Find** button to locate a specific entry based on the port number selected.

Click the **Clear** button to clear all the information entered in the fields.

Click the **View All** button to display all the existing entries.

MAC-based Access Control (MAC)

MAC-based access control is a method to authenticate and authorize access using either a port or host. For port-based MAC-based access control, the method decides port access rights, while for host-based MAC-based access control, the method determines the MAC access rights.

A MAC user must be authenticated before being granted access to a network. Both local authentication and remote RADIUS server authentication methods are supported. In MAC-based access control, MAC user information in a local database or a RADIUS server database is searched for authentication. Following the authentication result, users achieve different levels of authorization.

Notes about MAC-based Access Control

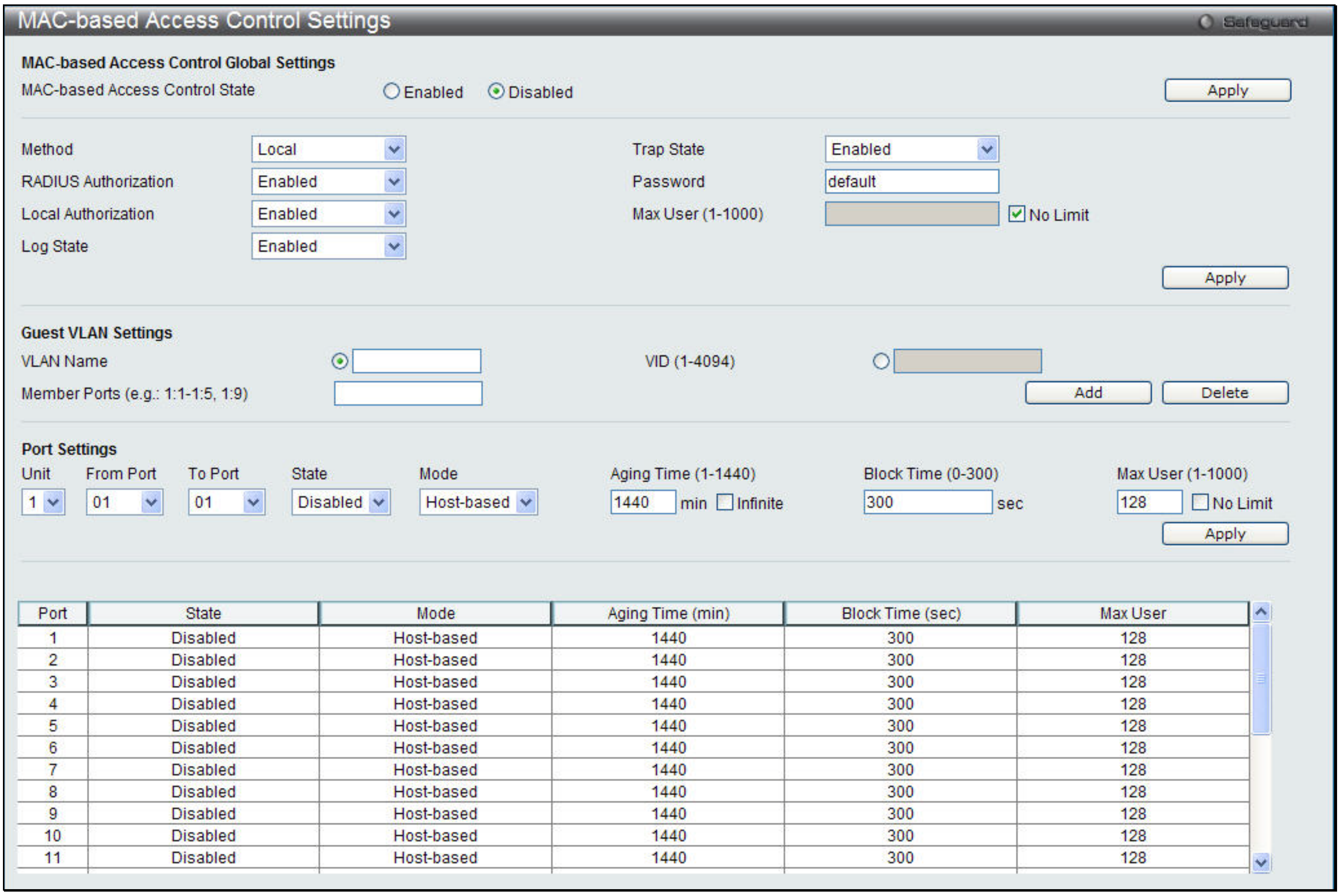
There are certain limitations and regulations regarding MAC-based access control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. If a port is granted clearance for a MAC address in a VLAN that is not a Guest VLAN, other MAC addresses on that port must be authenticated for access and otherwise will be blocked by the Switch.
3. Ports that have been enabled for Link Aggregation and Port Security cannot be enabled for MAC-based Authentication.
4. Ports that have been enabled for GVRP cannot be enabled for Guest VLAN.

MAC-based Access Control Settings

This window is used to set the parameters for the MAC-based access control function on the Switch. The user can set the running state, method of authentication, RADIUS password, view the Guest VLAN configuration to be associated with the MAC-based access control function of the Switch, and configure ports to be enabled or disabled for the MAC-based access control feature of the Switch. Please remember, ports enabled for certain other features, listed previously, and cannot be enabled for MAC-based access control.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings** as shown below:



MAC-based Access Control Global Settings

MAC-based Access Control State ○ Enabled ● Disabled

Method: Local

RADIUS Authorization: Enabled

Local Authorization: Enabled

Log State: Enabled

Trap State: Enabled

Password: default

Max User (1-1000): ☑ No Limit

Guest VLAN Settings

VLAN Name ●

VID (1-4094) ○

Member Ports (e.g.: 1:1-1:5, 1:9)

Port Settings

Unit	From Port	To Port	State	Mode	Aging Time (1-1440)	Block Time (0-300)	Max User (1-1000)
1	01	01	Disabled	Host-based	1440 min ☐ Infinite	300 sec	128 ☐ No Limit

Port	State	Mode	Aging Time (min)	Block Time (sec)	Max User
1	Disabled	Host-based	1440	300	128
2	Disabled	Host-based	1440	300	128
3	Disabled	Host-based	1440	300	128
4	Disabled	Host-based	1440	300	128
5	Disabled	Host-based	1440	300	128
6	Disabled	Host-based	1440	300	128
7	Disabled	Host-based	1440	300	128
8	Disabled	Host-based	1440	300	128
9	Disabled	Host-based	1440	300	128
10	Disabled	Host-based	1440	300	128
11	Disabled	Host-based	1440	300	128

Figure 8-33 MAC-based Access Control Settings window

The fields that can be configured are described below:

Parameter	Description
MAC-based Access Control State	Toggle to globally enable or disable the MAC-based access control function on the Switch.
Method	Use this drop-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: *Local* – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based access control. This MAC address list can be configured in the MAC-based access control Local Database Settings window. *RADIUS* – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based access control. Remember, the MAC list must be previously set on the RADIUS server.
RADIUS Authorization	Use the drop-down menu to enable or disable the use of RADIUS Authorization.
Local Authorization	Use the drop-down menu to enable or disable the use of Local Authorization.
Log State	Use the drop-down menu to enable or disable log state.
Trap State	Use the drop-down menu to enable or disable trap state.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
Max User (1-1000)	Enter the maximum amount of users of the Switch. Tick the **No Limit** check box to have unlimited users.
VLAN Name	Enter the name of the previously configured Guest VLAN being used for this function.
VID (1-4094)	Click the radio button and enter a Guest VLAN ID.

Member Ports	Enter the list of ports that have been configured for the Guest VLAN.
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured for MAC-based access control.
State	Use this drop-down menu to enable or disable MAC-based access control on the port or range of ports selected in the Port Settings section of this window.
Mode	Toggle between *Port-based* and *Host-based*.
Aging Time (1-1440)	Enter a value between *1* and *1440* minutes. The default is *1440*. To set this value to have no aging time, select the **Infinite** option.
Block Time (0-300)	Enter a value between *0* and *300* seconds. The default is *300*.
Max User (1-1000)	Enter the maximum user used for this configuration. When **No Limit** is selected, there will be no user limit applied to this rule.

Click the **Apply** button to accept the changes made for each individual section.

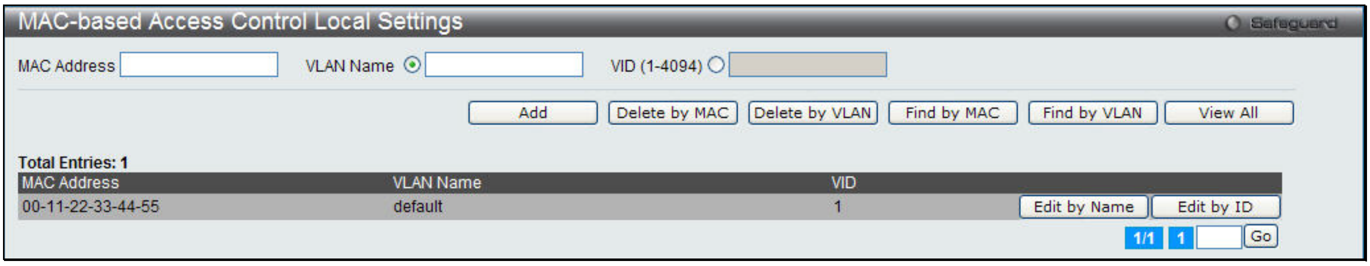
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

MAC-based Access Control Local Settings

Users can set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this window, it will be placed in the VLAN associated with it here. The Switch administrator may enter up to 128 MAC addresses to be authenticated using the local method configured here.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings** as shown below:



Total Entries: 1

MAC Address	VLAN Name	VID
00-11-22-33-44-55	default	1

Figure 8-34 MAC-based Access Control Local Settings window

The fields that can be configured are described below:

Parameter	Description
MAC address	Enter the MAC address that will be added to the local authentication list here.
VLAN Name	Enter the VLAN name of the corresponding MAC address here.
VID (1-4094)	Enter the VLAN ID of the corresponding MAC address here.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete by MAC** button to remove the specific entry based on the MAC address entered.

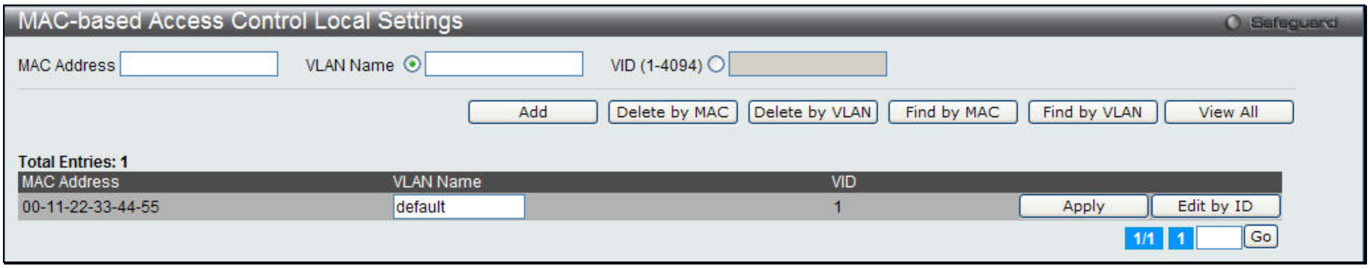
Click the **Delete by VLAN** button to remove the specific entry based on the VLAN name or ID entered.

Click the **Find by MAC** button to locate a specific entry based on the MAC address entered.

Click the **Find by VLAN** button to locate a specific entry based on the VLAN name or ID entered.

Click the **View All** button to display all the existing entries.

To change the selected MAC address' VLAN Name, the user can click the **Edit by Name** button.

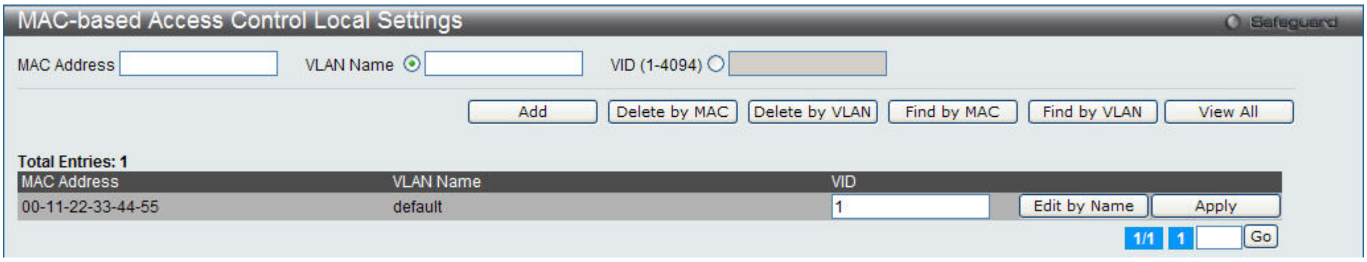

MAC-based Access Control Local Settings
Safeguard
MAC Address
VLAN Name ●
VID (1-4094) ○
Add
Delete by MAC
Delete by VLAN
Find by MAC
Find by VLAN
View All
Apply
Edit by ID
1/1
1
Go

Total Entries: 1

MAC Address	VLAN Name	VID
00-11-22-33-44-55	default	1

Figure 8-35 MAC-based Access Control Local Settings – Edit by Name window

To change the selected MAC address’ VID value, the user can click the **Edit by ID** button.


MAC-based Access Control Local Settings
Safeguard
MAC Address
VLAN Name ●
VID (1-4094) ○
Add
Delete by MAC
Delete by VLAN
Find by MAC
Find by VLAN
View All
Edit by Name
Apply
1/1
1
Go

Total Entries: 1

MAC Address	VLAN Name	VID
00-11-22-33-44-55	default	1

Figure 8-36 MAC-based Access Control Local Settings – Edit by ID window

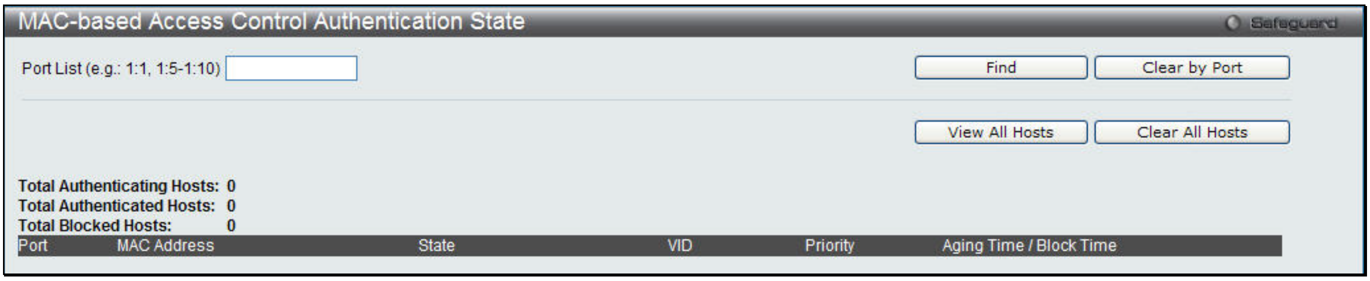
Click the **Apply** button to accept the changes made.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

MAC-based Access Control Authentication State

Users can display MAC-based access control Authentication State information.

To view this window, click **Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State** as shown below:


MAC-based Access Control Authentication State
Safeguard
Port List (e.g.: 1:1, 1:5-1:10)
Find
Clear by Port
View All Hosts
Clear All Hosts

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Blocked Hosts: 0

Port	MAC Address	State	VID	Priority	Aging Time / Block Time

Figure 8-37 MAC-based Access Control Authentication State window

To display MAC-based access control Authentication State information, enter a port number in the space provided and then click the **Find** button.

Click the **Clear by Port** button to clear all the information linked to the port number entered.

Click the **View All Hosts** button to display all the existing hosts.

Click the **Clear All hosts** button to clear out all the existing hosts.

Web-based Access Control (WAC)

Web-based Authentication Login is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch. The authentication process uses the HTTP or HTTPS protocol. The Switch enters the authenticating stage when users attempt to browse Web pages (e.g., http://www.dlink.com) through a Web browser. When the Switch detects HTTP or HTTPS packets and this port is un-authenticated, the Switch will launch a pop-up user name and password window to query users. Users are not able to access the Internet until the authentication process is passed.

The Switch can be the authentication server itself and do the authentication based on a local database, or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server. The client user initiates the authentication process of WAC by attempting to gain Web access.

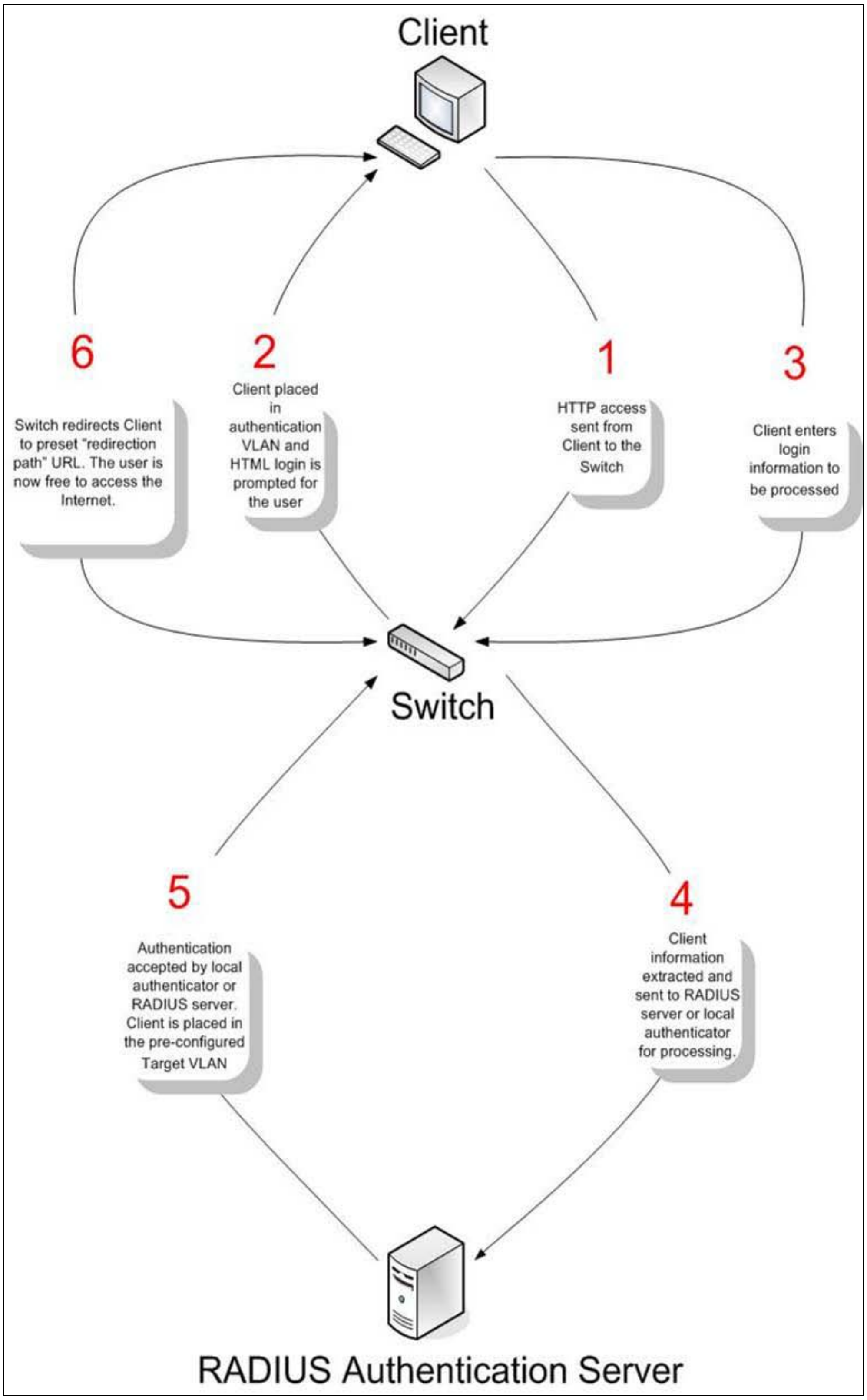
D-Link's implementation of WAC uses a virtual IP that is exclusively used by the WAC function and is not known by any other modules of the Switch. In fact, to avoid affecting a Switch's other features, WAC will only use a virtual IP address to communicate with hosts. Thus, all authentication requests must be sent to a virtual IP address but not to the IP address of the Switch's physical interface.

Virtual IP works like this, when a host PC communicates with the WAC Switch through a virtual IP, the virtual IP is transformed into the physical IPIF (IP interface) address of the Switch to make the communication possible. The host PC and other servers' IP configurations do not depend on the virtual IP of WAC. The virtual IP does not respond to any ICMP packets or ARP requests, which means it is not allowed to configure a virtual IP on the same subnet as the Switch's IPIF (IP interface) or the same subnet as the host PCs' subnet.

As all packets to a virtual IP from authenticated and authenticating hosts will be trapped to the Switch's CPU, if the virtual IP is the same as other servers or PCs, the hosts on the WAC-enabled ports cannot communicate with the server or PC which really own the IP address. If the hosts need to access the server or PC, the virtual IP cannot be the same as the one of the server or PC. If a host PC uses a proxy to access the Web, to make the authentication work properly the user of the PC should add the virtual IP to the exception of the proxy configuration. Whether or not a virtual IP is specified, users can access the WAC pages through the Switch's system IP. When a virtual IP is not specified, the authenticating Web request will be redirected to the Switch's system IP.

The Switch's implementation of WAC features a user-defined port number that allows the configuration of the TCP port for either the HTTP or HTTPS protocols. This TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to the CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80 and the default port number for HTTPS is 443. If no protocol is specified, the default protocol is HTTP.

The following diagram illustrates the basic six steps all parties go through in a successful Web Authentication process:


Client
1
HTTP access sent from Client to the Switch
2
Client placed in authentication VLAN and HTML login is prompted for the user
3
Client enters login information to be processed
4
Client information extracted and sent to RADIUS server or local authenticator for processing.
5
Authentication accepted by local authenticator or RADIUS server. Client is placed in the pre-configured Target VLAN
6
Switch redirects Client to preset "redirection path" URL. The user is now free to access the Internet.
Switch
RADIUS Authentication Server

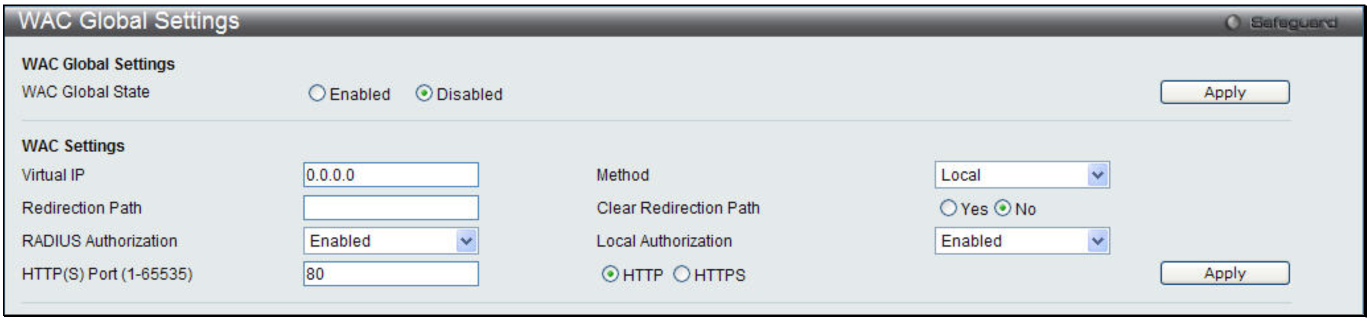
Conditions and Limitations

1. If the client is utilizing DHCP to attain an IP address, the authentication VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
2. Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
3. If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling Web Authentication on the Switch.

WAC Global Settings

Users can configure the Switch for the Web-based access control function.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Global Settings** as shown below:



WAC Global Settings

WAC Global State ○ Enabled ● Disabled

WAC Settings

Virtual IP: 0.0.0.0

Method: Local

Redirection Path:

Clear Redirection Path: ○ Yes ● No

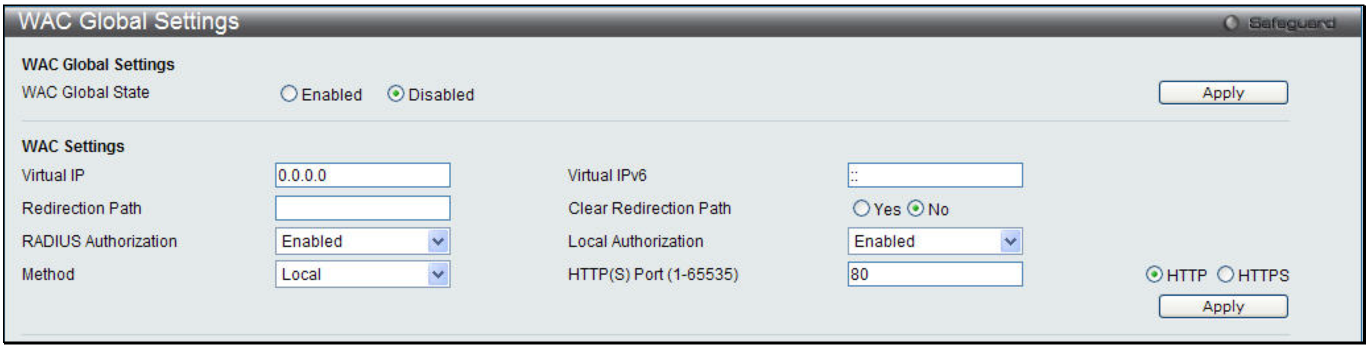
RADIUS Authorization: Enabled

Local Authorization: Enabled

HTTP(S) Port (1-65535): 80

● HTTP ○ HTTPS

Figure 8-38 WAC Global Settings window (SI mode Only)



WAC Global Settings

WAC Global State ○ Enabled ● Disabled

WAC Settings

Virtual IP: 0.0.0.0

Virtual IPv6: ::

Redirection Path:

Clear Redirection Path: ○ Yes ● No

RADIUS Authorization: Enabled

Local Authorization: Enabled

Method: Local

HTTP(S) Port (1-65535): 80

● HTTP ○ HTTPS

Figure 8-39 WAC Global Settings window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
WAC Global State	Use this selection menu to either enable or disable the Web Authentication on the Switch.
Virtual IP	Enter a virtual IP address. This is used to accept authentication requests from unauthenticated hosts. Only requests sent to this IP will get a correct response.
Virtual IPv6 (EI Mode Only)	Enter a virtual IPv6 address. This is used to accept authentication requests from unauthenticated hosts. Only requests sent to this IP will get a correct response.
Redirection Path	Enter the URL of the website that authenticated users placed in the VLAN are directed to once authenticated.
Clear Redirection Path	The user can enable or disable this option to clear the redirection path.
RADIUS Authorization	The user can enable or disable this option to enable RADIUS Authorization or not.
Local Authorization	The user can enable or disable this option to enable Local Authorization or not.
Method	Use this drop-down menu to choose the authenticator for Web-based Access Control. The user may choose: *Local* – Choose this parameter to use the local authentication method of the Switch as the authenticating method for users trying to access the network via the switch. This is, in fact, the username and password to access the Switch configured using the WAC User Settings window (**Security** > **Web-based Access Control** > **WAC User Settings**) seen below. *RADIUS* – Choose this parameter to use a remote RADIUS server as the authenticating method for users trying to access the network via the switch. This

	RADIUS server must have already been pre-assigned by the administrator using the Authentication RADIUS Server Settings window (**Security** > **RADIUS** > **Authentication RADIUS Server Settings**).
HTTP(S) Port (1-65535)	Enter a HTTP port number. Port *80* is the default. *HTTP* – Specifies that the TCP port will run the WAC HTTP protocol. The default value is 80. HTTP port cannot run at TCP port 443. *HTTPS* – Specifies that the TCP port will run the WAC HTTPS protocol. The default value is 443. HTTPS cannot run at TCP port 80.

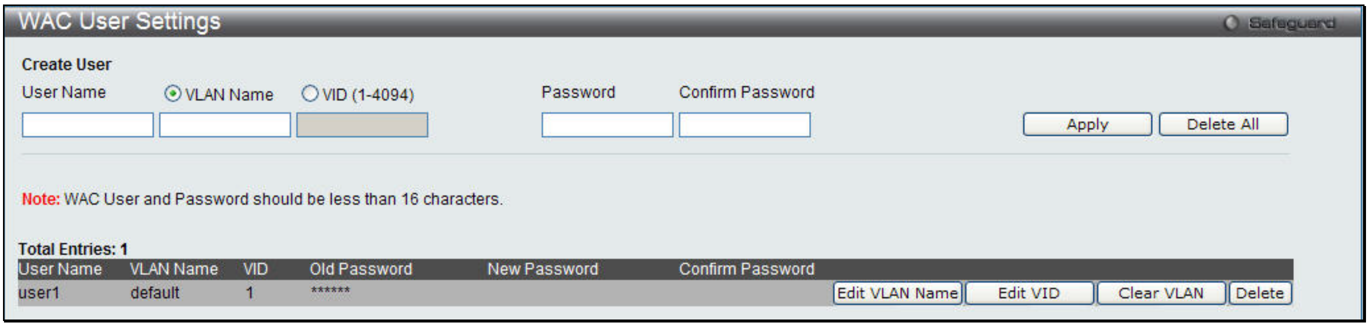
Click the **Apply** button to accept the changes made for each individual section.

NOTE: A successful authentication should direct the client to the stated web page. If the client does not reach this web page, yet does not receive a **Fail!** Message, the client will already be authenticated and therefore should refresh the current browser window or attempt to open a different web page.

WAC User Settings

Users can view and set local database user accounts for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC User Settings** as shown below:



Note: WAC User and Password should be less than 16 characters.

Total Entries: 1

User Name	VLAN Name	VID	Old Password	New Password	Confirm Password
user1	default	1	******		

Figure 8-40 WAC User Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user name of up to 15 alphanumeric characters of the guest wishing to access the Web through this process. This field is for administrators who have selected *Local* as their Web-based authenticator.
VLAN Name	Click the button and enter a VLAN Name in this field.
VID (1-4094)	Click the button and enter a VID in this field.
Password	Enter the password the administrator has chosen for the selected user. This field is case-sensitive and must be a complete alphanumeric string. This field is for administrators who have selected *Local* as their Web-based authenticator.
Confirm Password	Retype the password entered in the previous field.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit VLAN Name** button to re-configure the specific entry’s VLAN Name.

Click the **Edit VID** button to re-configure the specific entry’s VLAN ID.

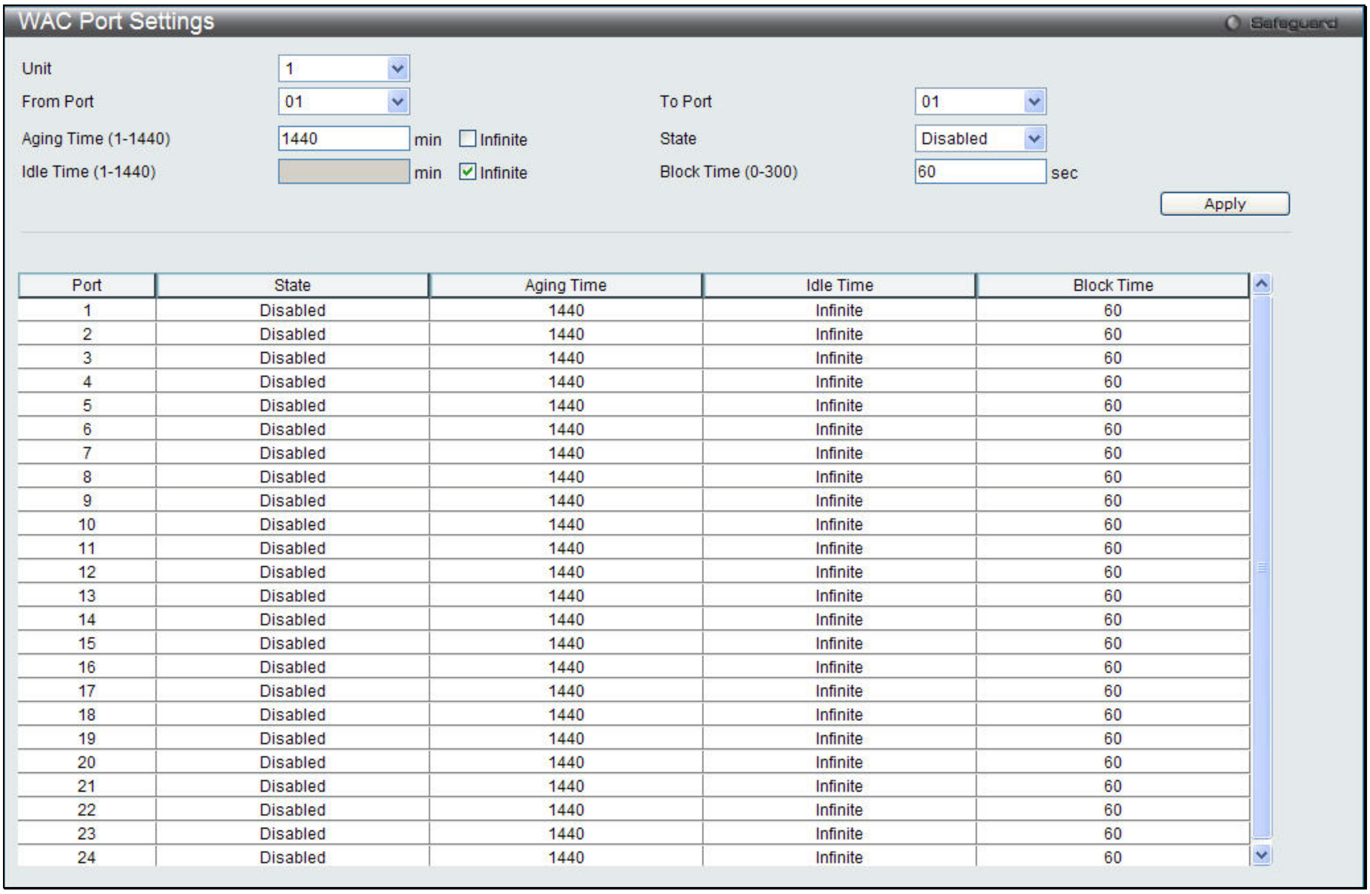
Click the **Clear VLAN** button to remove the VLAN information from the specific entry.

Click the **Delete** button to remove the specific entry.

WAC Port Settings

Users can view and set port configurations for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Port Settings** as shown below:



Unit: 1

From Port: 01

To Port: 01

Aging Time (1-1440): 1440 min ☐ Infinite

State: Disabled

Idle Time (1-1440): min ☑ Infinite

Block Time (0-300): 60 sec

Port	State	Aging Time	Idle Time	Block Time
1	Disabled	1440	Infinite	60
2	Disabled	1440	Infinite	60
3	Disabled	1440	Infinite	60
4	Disabled	1440	Infinite	60
5	Disabled	1440	Infinite	60
6	Disabled	1440	Infinite	60
7	Disabled	1440	Infinite	60
8	Disabled	1440	Infinite	60
9	Disabled	1440	Infinite	60
10	Disabled	1440	Infinite	60
11	Disabled	1440	Infinite	60
12	Disabled	1440	Infinite	60
13	Disabled	1440	Infinite	60
14	Disabled	1440	Infinite	60
15	Disabled	1440	Infinite	60
16	Disabled	1440	Infinite	60
17	Disabled	1440	Infinite	60
18	Disabled	1440	Infinite	60
19	Disabled	1440	Infinite	60
20	Disabled	1440	Infinite	60
21	Disabled	1440	Infinite	60
22	Disabled	1440	Infinite	60
23	Disabled	1440	Infinite	60
24	Disabled	1440	Infinite	60

Figure 8-41 WAC Port Settings window

The fields that can be configured are described below:

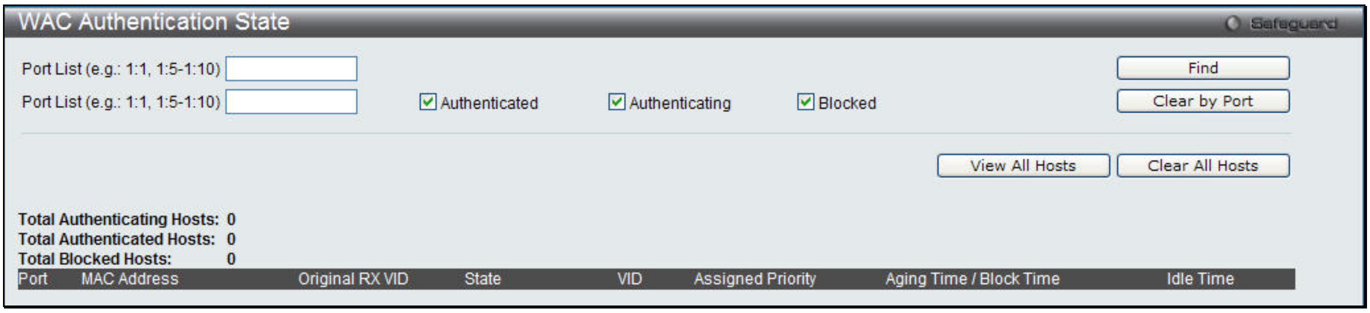
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be enabled as WAC ports.
Aging Time (1-1440)	This parameter specifies the time period during which an authenticated host will remain in the authenticated state. Enter a value between *1*and *1440* minutes. Tick the **Infinite** check box to indicate the authenticated host will never age out on the port. The default value is *1440* minutes (24 hours).
State	Use this drop-down menu to enable the configured ports as WAC ports.
Idle Time (1-1440)	If there is no traffic during the Idle Time parameter, the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. Tick the **Infinite** check box to indicate the Idle state of the authenticated host on the port will never be checked. The default value is *infinite*.
Block Time (0-300)	This parameter is the period of time a host will be blocked if it fails to pass authentication. Enter a value between *0* and *300* seconds. The default value is *60* seconds.

Click the **Apply** button to accept the changes made.

WAC Authentication State

Users can view and delete the hosts for Web authentication.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Authentication State** as shown below:


WAC Authentication State
Safeguard
Port List (e.g.: 1:1, 1:5-1:10)
Port List (e.g.: 1:1, 1:5-1:10)
☑ Authenticated
☑ Authenticating
☑ Blocked
Find
Clear by Port
View All Hosts
Clear All Hosts
Port
MAC Address
Original RX VID
State
VID
Assigned Priority
Aging Time / Block Time
Idle Time

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Blocked Hosts: 0

Figure 8-42 WAC Authentication State window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter the desired range of ports and tick the appropriate check box(s), Authenticated, Authenticating, and Blocked.
Authenticated	Tick this check box to clear all authenticated users for a port.
Authenticating	Tick this check box to clear all authenticating users for a port.
Blocked	Tick this check box to clear all blocked users for a port.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear by Port** button to remove entry based on the port list entered.

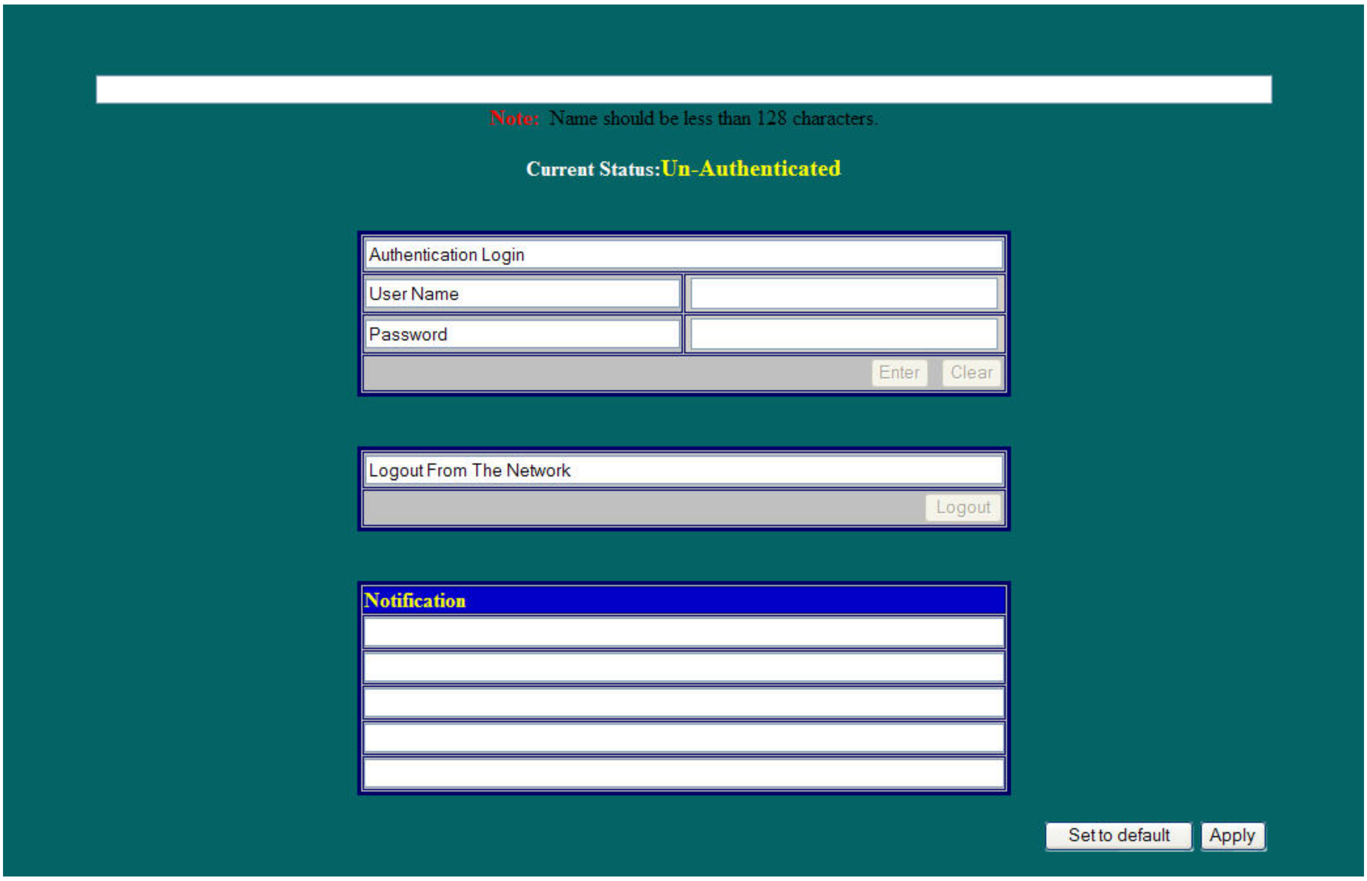
Click the **View All Hosts** button to display all the existing entries.

Click the **Clear All Hosts** button to remove all the entries listed.

WAC Customize Page

This window is used to customize the authenticate page elements.

To view this window, click **Security > Web-based Access Control (WAC) > WAC Customize Page** as shown below:



Note: Name should be less than 128 characters.

Current Status:Un-Authenticated

Authentication Login	
User Name	
Password	

Figure 8-43 WAC Customize Page window

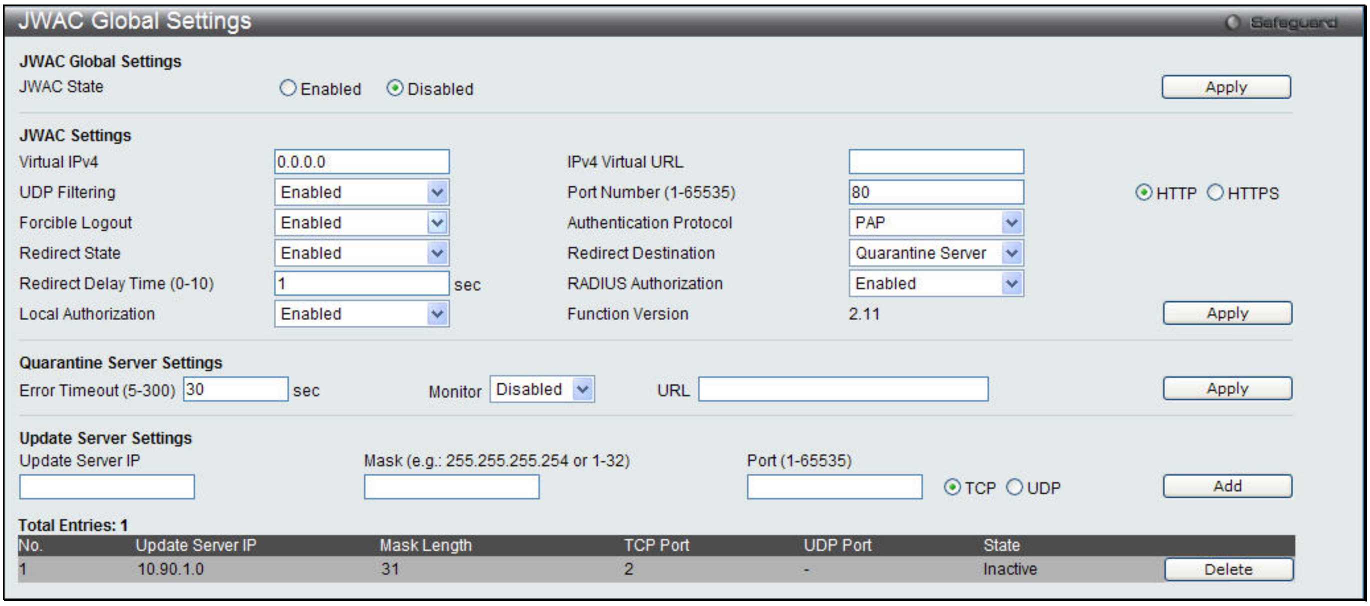
Complete the WAC authentication information on this window to set the WAC page settings. Click the **Apply** button to implement the changes made. Click the **Set to default** button to go back to the default settings of all elements.

Japanese Web-based Access Control (JWAC)

JWAC Global Settings

This window is used to enable and configure Japanese Web-based Access Control on the Switch. JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the Switch. For the second stage, the authentication is similar to Web Authentication, except that there is no port VLAN membership change by JWAC after a host passes authentication. JWAC and WAC can share the same RADIUS server.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings** as shown below:



JWAC Global Settings

JWAC State ○ Enabled ● Disabled

JWAC Settings

Virtual IPv4: 0.0.0.0
IPv4 Virtual URL:
UDP Filtering: Enabled
Port Number (1-65535): 80 ● HTTP ○ HTTPS
Forcible Logout: Enabled
Authentication Protocol: PAP
Redirect State: Enabled
Redirect Destination: Quarantine Server
Redirect Delay Time (0-10): 1 sec
RADIUS Authorization: Enabled
Local Authorization: Enabled
Function Version: 2.11

Quarantine Server Settings

Error Timeout (5-300): 30 sec
Monitor: Disabled
URL:

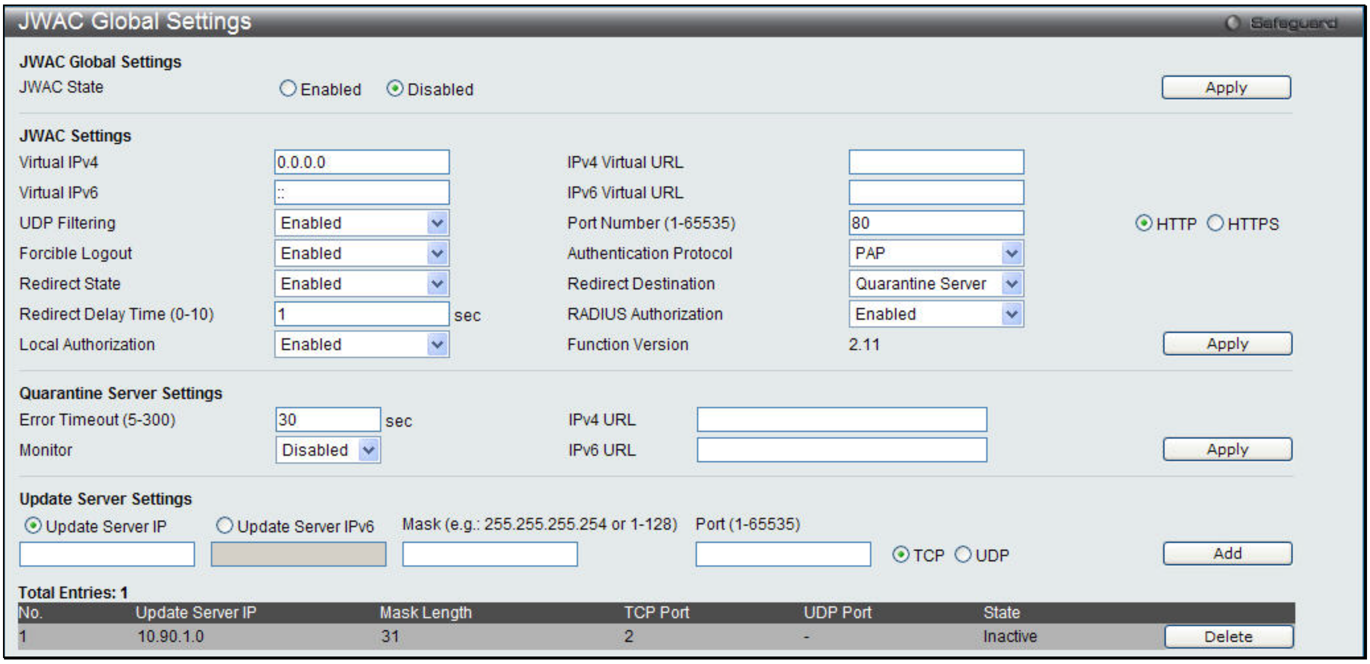
Update Server Settings

Update Server IP:
Mask (e.g.: 255.255.255.254 or 1-32):
Port (1-65535): ● TCP ○ UDP

Total Entries: 1

No.	Update Server IP	Mask Length	TCP Port	UDP Port	State	
1	10.90.1.0	31	2	-	Inactive	Delete

Figure 8-44 JWAC Global Settings (SI Mode Only)



JWAC Global Settings

JWAC State ○ Enabled ● Disabled

JWAC Settings

Virtual IPv4: 0.0.0.0
IPv4 Virtual URL:
Virtual IPv6: ::
IPv6 Virtual URL:
UDP Filtering: Enabled
Port Number (1-65535): 80 ● HTTP ○ HTTPS
Forcible Logout: Enabled
Authentication Protocol: PAP
Redirect State: Enabled
Redirect Destination: Quarantine Server
Redirect Delay Time (0-10): 1 sec
RADIUS Authorization: Enabled
Local Authorization: Enabled
Function Version: 2.11

Quarantine Server Settings

Error Timeout (5-300): 30 sec
IPv4 URL:
Monitor: Disabled
IPv6 URL:

Update Server Settings

● Update Server IP ○ Update Server IPv6
Mask (e.g.: 255.255.255.254 or 1-128):
Port (1-65535): ● TCP ○ UDP

Total Entries: 1

No.	Update Server IP	Mask Length	TCP Port	UDP Port	State	
1	10.90.1.0	31	2	-	Inactive	Delete

Figure 8-45 JWAC Global Settings window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
JWAC State	Click to enable or disable JWAC on the Switch.
Virtual IPv4	Enter the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. The Virtual IP address of JWAC is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. **NOTE:** This IP does not respond to ARP requests or ICMP packets.
IPv4 Virtual URL	Enter the IPv4 Virtual URL used.
Virtual IPv6 (EI Mode Only)	Enter the JWAC Virtual IPv6 address that is used to accept authentication requests from an unauthenticated host.
IPv6 Virtual URL (EI Mode Only)	Enter the IPv6 Virtual URL used.

UDP Filtering	Use the drop-down menu to enable or disable JWAC UDP Filtering. When UDP Filtering is *Enabled*, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.
Port Number (1-65535)	Enter the TCP port that the JWAC Switch listens to and uses to finish the authenticating process.
Forcible Logout	Use the drop-down menu to enable or disable JWAC Forcible Logout. When Forcible Logout is *Enabled*, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
Authentication Protocol	Use the drop-down menu to select the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include *Local*, *EAP MD5*, *PAP*, *CHAP*, *MS CHAP*, and *MS CHAPv2*.
Redirect State	Use the drop-down menu to enable or disable JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. **NOTE:** When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	Use the drop-down menu to select the destination before an unauthenticated host is redirected to either the *Quarantine Server* or the *JWAC Login Page*.
Redirect Delay Time (0-10)	Enter the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between *0* and *10* seconds. A value of *0* indicates no delay in the redirect.
RADIUS Authorization	Use the drop-down menu to enable or disable this option to enable RADIUS Authorization or not.
Local Authorization	Use the drop-down menu to enable or disable this option to enable Local Authorization or not.
Error Timeout (5-300)	Enter the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between *5* and *300* seconds.
Monitor	Use the drop-down menu to enable or disable the JWAC Quarantine Server Monitor. When *Enabled*, the JWAC Switch will monitor the Quarantine Server to ensure the server is okay. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.
URL (SI Mode Only)	Enter the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
IPv4 URL (EI Mode Only)	Enter the JWAC Quarantine Server IPv4 URL.
IPv6 URL (EI Mode Only)	Enter the JWAC Quarantine Server IPv6 URL.
Update Server IP	Enter the Update Server IP address.
Update Server IPv6 (EI Mode Only)	Enter the Update Server IPv6 address.
Mask	This parameter specifies the Server IP net mask.

Port (1-65535)	Enter the port number used by the Update Server.
TCP	Click the radio button to use TCP port.
UDP	Click the radio button to use UDP port.

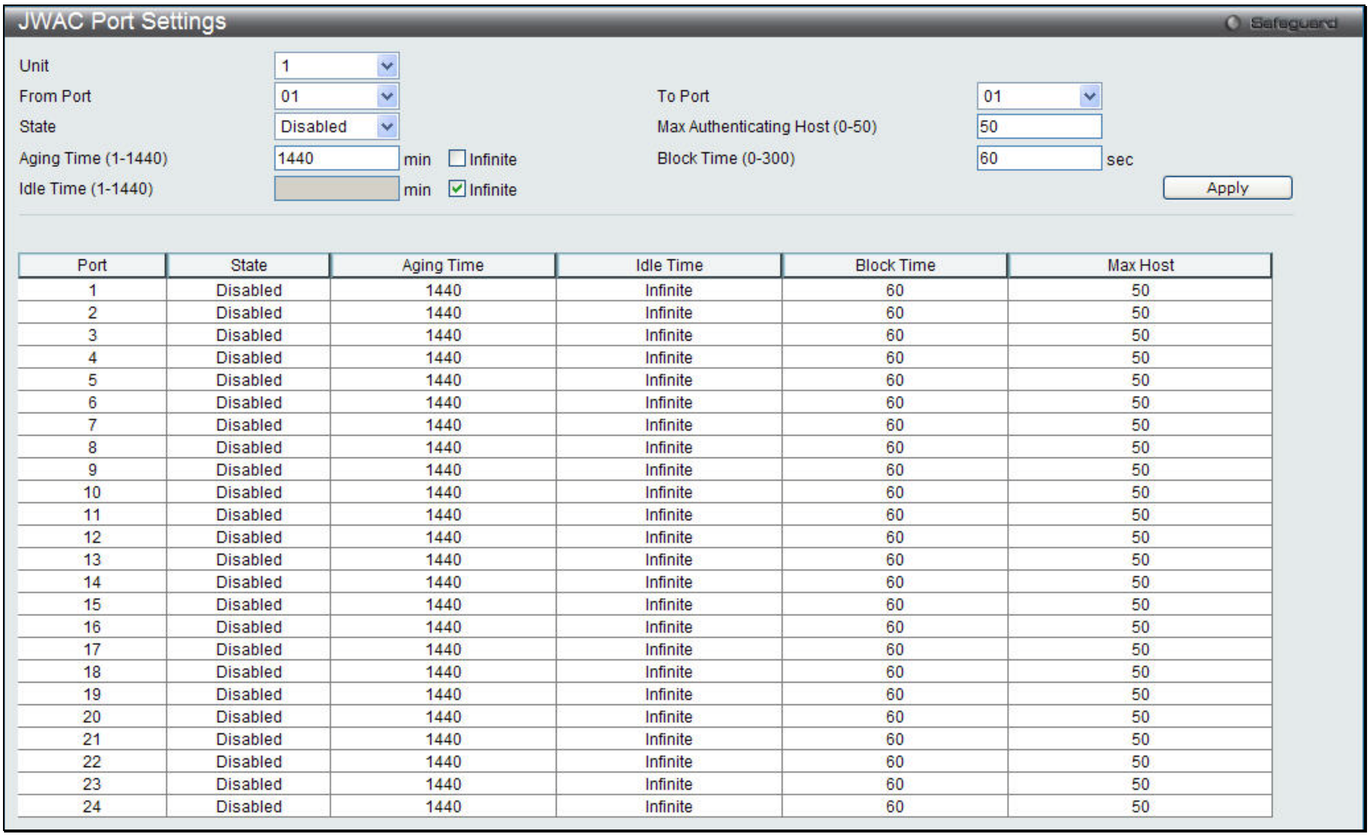
Click the **Apply** button to accept the changes made for each individual section.

Click the **Add** button to add a new entry based on the information entered.

JWAC Port Settings

This window is used to configure JWAC port settings for the Switch.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Port Settings** as shown below:



Unit: 1

From Port: 01

To Port: 01

State: Disabled

Max Authenticating Host (0-50): 50

Aging Time (1-1440): 1440 min ☐ Infinite

Block Time (0-300): 60 sec

Idle Time (1-1440): min ☑ Infinite

Port	State	Aging Time	Idle Time	Block Time	Max Host
1	Disabled	1440	Infinite	60	50
2	Disabled	1440	Infinite	60	50
3	Disabled	1440	Infinite	60	50
4	Disabled	1440	Infinite	60	50
5	Disabled	1440	Infinite	60	50
6	Disabled	1440	Infinite	60	50
7	Disabled	1440	Infinite	60	50
8	Disabled	1440	Infinite	60	50
9	Disabled	1440	Infinite	60	50
10	Disabled	1440	Infinite	60	50
11	Disabled	1440	Infinite	60	50
12	Disabled	1440	Infinite	60	50
13	Disabled	1440	Infinite	60	50
14	Disabled	1440	Infinite	60	50
15	Disabled	1440	Infinite	60	50
16	Disabled	1440	Infinite	60	50
17	Disabled	1440	Infinite	60	50
18	Disabled	1440	Infinite	60	50
19	Disabled	1440	Infinite	60	50
20	Disabled	1440	Infinite	60	50
21	Disabled	1440	Infinite	60	50
22	Disabled	1440	Infinite	60	50
23	Disabled	1440	Infinite	60	50
24	Disabled	1440	Infinite	60	50

Figure 8-46 JWAC Port Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be enabled as JWAC ports.
State	Use this drop-down menu to enable the configured ports as JWAC ports.
Max Authenticating Host (0-50)	Enter the maximum number of host that process authentication on each port at the same time.
Aging Time (1-1440)	This parameter specifies the time period during which an authenticated host will remain in the authenticated state. Enter a value between *1*and *1440* minutes. Tick the **Infinite** check box to indicate the authenticated host will never age out on the port. The default value is *1440* minutes (24 hours).
Idle Time (1-1440)	If there is no traffic during the Idle Time parameter, the host will be moved back to the unauthenticated state. Enter a value between *1* and *1440* minutes. Tick the **Infinite**

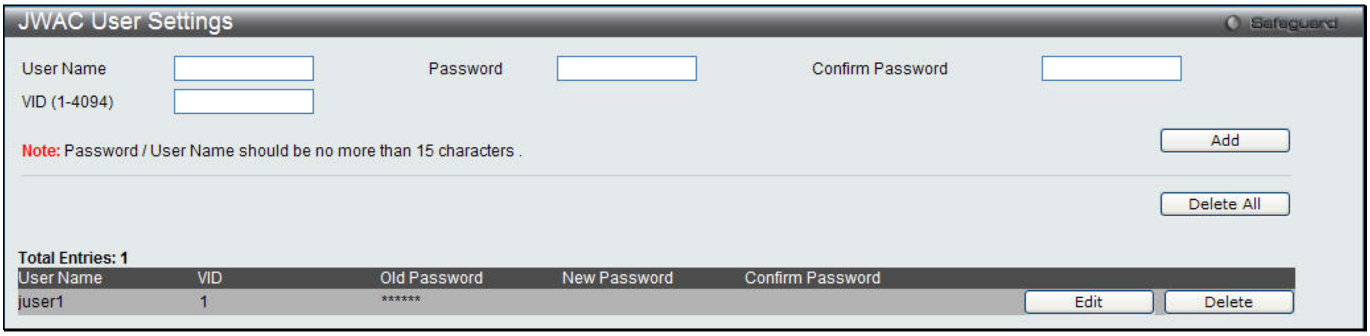
	check box to indicate the Idle state of the authenticated host on the port will never be checked. The default value is *infinite*.
Block Time (0-300)	This parameter is the period of time a host will be blocked if it fails to pass authentication. Enter a value between *0* and *300* seconds. The default value is *60* seconds.

Click the **Apply** button to accept the changes made.

JWAC User Settings

This window is used to configure JWAC user settings for the Switch.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC User Settings** as shown below:



Note: Password / User Name should be no more than 15 characters .

Total Entries: 1

User Name	VID	Old Password	New Password	Confirm Password		
juser1	1	******			Edit	Delete

Figure 8-47 JWAC User Settings window

The fields that can be configured are described below:

Parameter	Description
User Name	Enter the user name of up to 15 alphanumeric characters of the guest wishing to access the Web through this process. This field is for administrators who have selected *Local* as their Web-based authenticator.
VID (1-4094)	Click the button and enter a VID in this field.
Password	Enter the password the administrator has chosen for the selected user. This field is case-sensitive and must be a complete alphanumeric string. This field is for administrators who have selected *Local* as their Web-based authenticator.
Confirm Password	Retype the password entered in the previous field.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

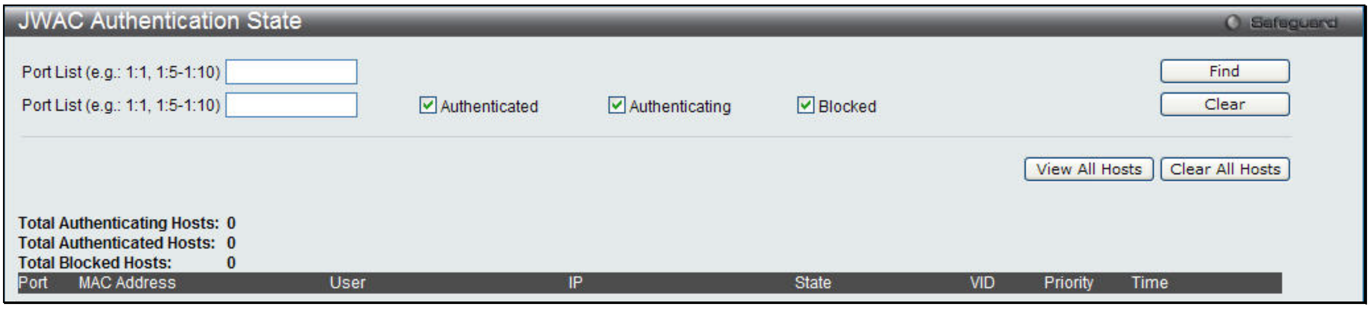
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

JWAC Authentication State

This window is used to display Japanese web-based access control host table information.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Authentication State** as shown below:



Port List (e.g.: 1:1, 1:5-1:10)

Port List (e.g.: 1:1, 1:5-1:10) ☑ Authenticated ☑ Authenticating ☑ Blocked

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Blocked Hosts: 0

Port	MAC Address	User	IP	State	VID	Priority	Time

Figure 8-48 JWAC Authentication State window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter the desired range of ports and tick the appropriate check box(s), Authenticated, Authenticating, and Blocked.
Authenticated	Tick this check box to clear all authenticated users for a port.
Authenticating	Tick this check box to clear all authenticating users for a port.
Blocked	Tick this check box to clear all blocked users for a port.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to remove entry based on the port list entered.

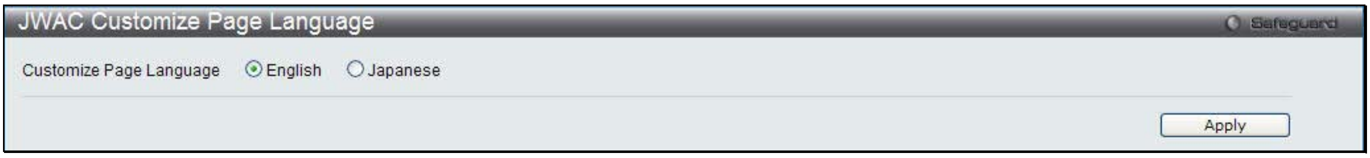
Click the **View All Hosts** button to display all the existing entries.

Click the **Clear All Hosts** button to remove all the entries listed.

JWAC Customize Page Language

This window is used to configure JWAC page language settings for the Switch. The current firmware supports either English or Japanese.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language** as shown below:



Customize Page Language ● English ○ Japanese

Figure 8-49 JWAC Customize Page Language window

The fields that can be configured are described below:

Parameter	Description
Customize Page Language	Click to select the language of JWAC Customize Page, either English or Japanese.

Click the **Apply** button to accept the changes made.

JWAC Customize Page

This window is used to configure JWAC page settings for the Switch.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page** as shown below:

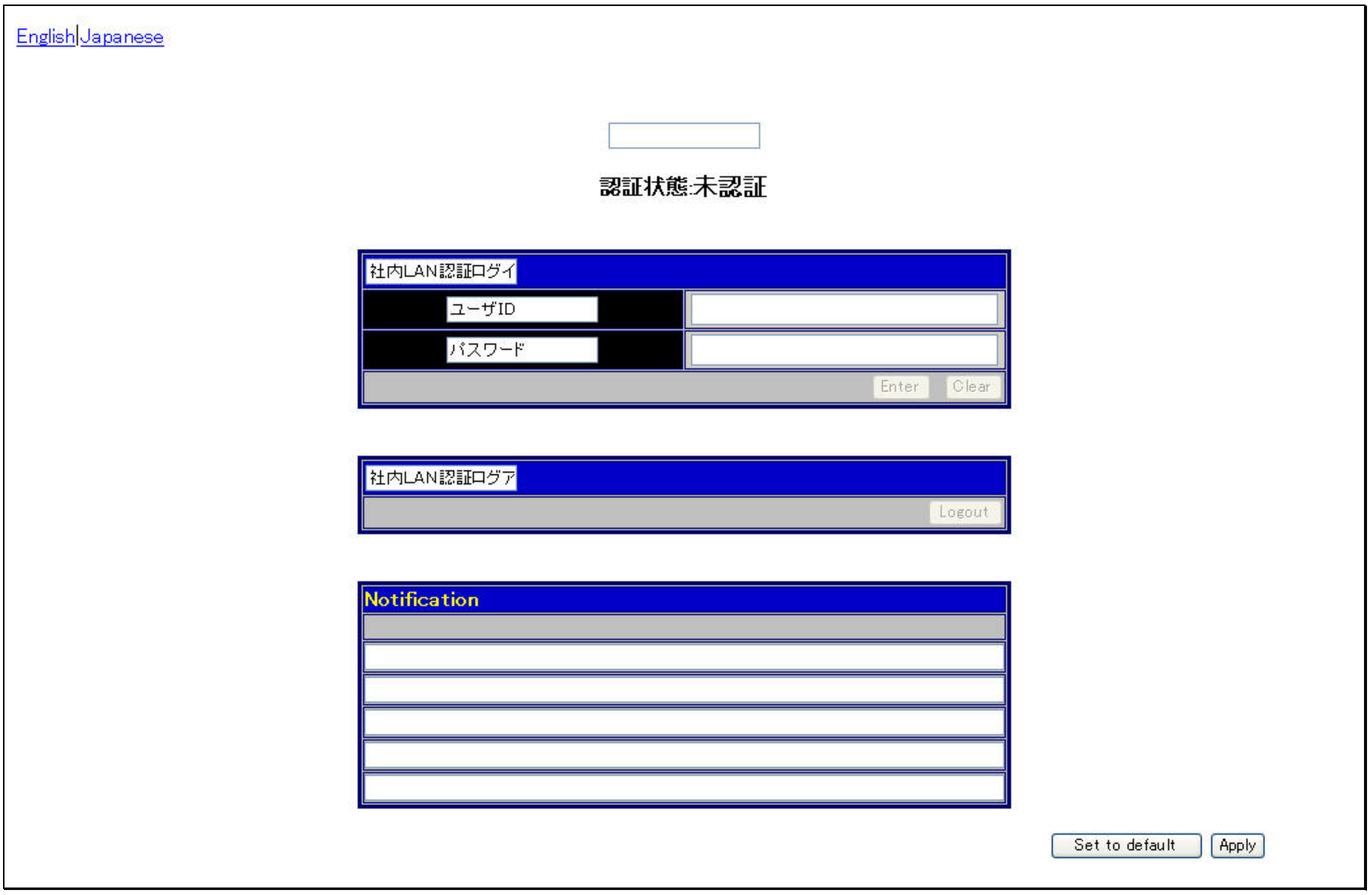

English|Japanese
認証状態:未認証
社内LAN認証ログイ
ユーザID
パスワード
Enter
Clear
社内LAN認証ログア
Logout
Notification
Set to default
Apply

Figure 8-50 JWAC Customize Page - Japanese window

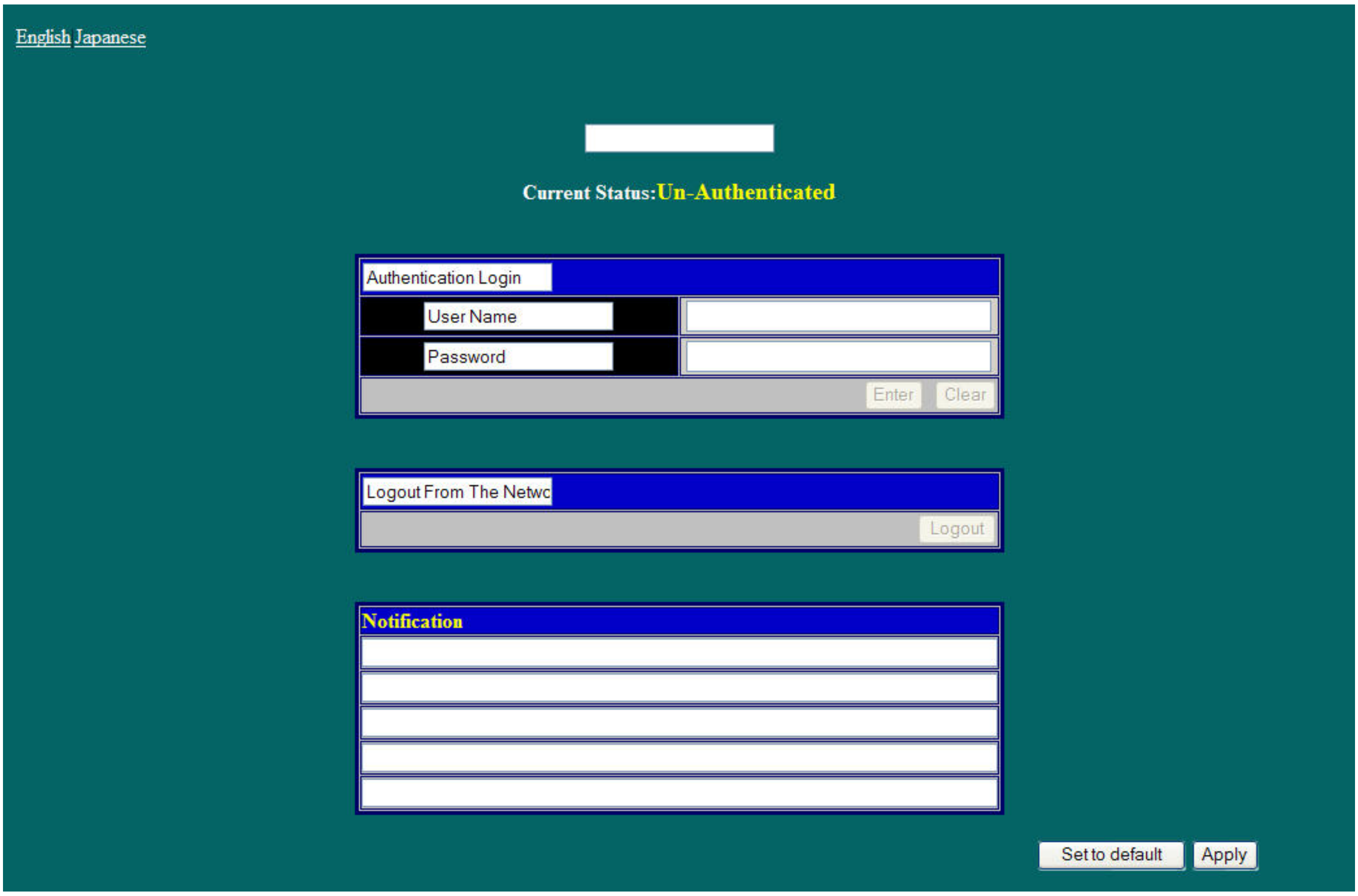

English Japanese
Current Status:Un-Authenticated
Authentication Login
User Name
Password
Enter
Clear
Logout From The Netwo
Logout
Notification
Set to default
Apply

Figure 8-51 JWAC Customize Page - English window

Complete the JWAC authentication information on this window to set the JWAC page settings. Click the **Apply** button to implement the changes made. Click the **Set to default** button to go back to the default settings of all elements.

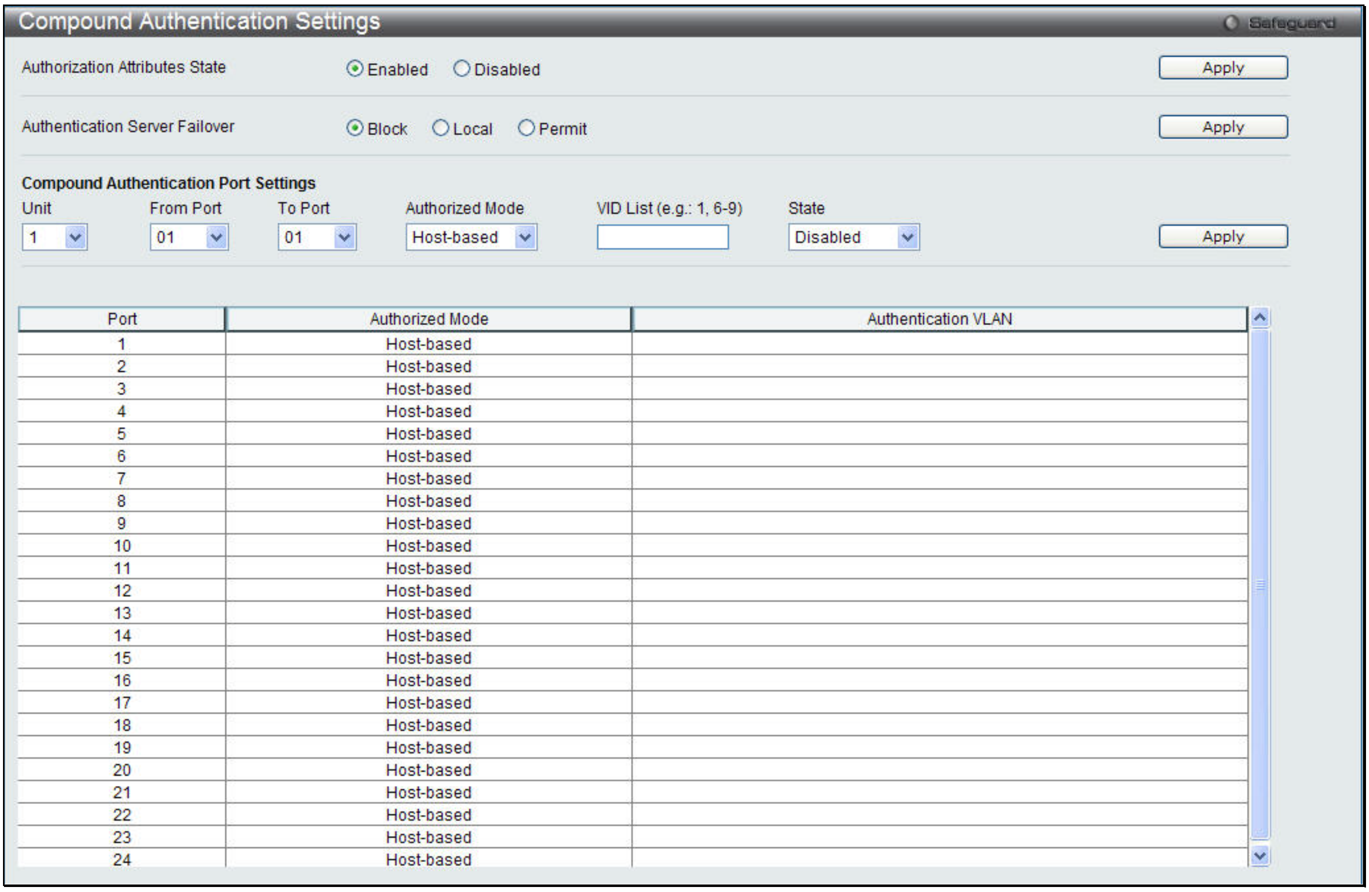
Compound Authentication

Compound Authentication settings allows for multiple authentication to be supported on the Switch.

Compound Authentication Settings

Users can configure Authorization Network State Settings and compound authentication methods for a port or ports on the Switch.

To view this window, click **Security > Compound Authentication > Compound Authentication Settings** as shown below:



Authorization Attributes State ● Enabled ○ Disabled

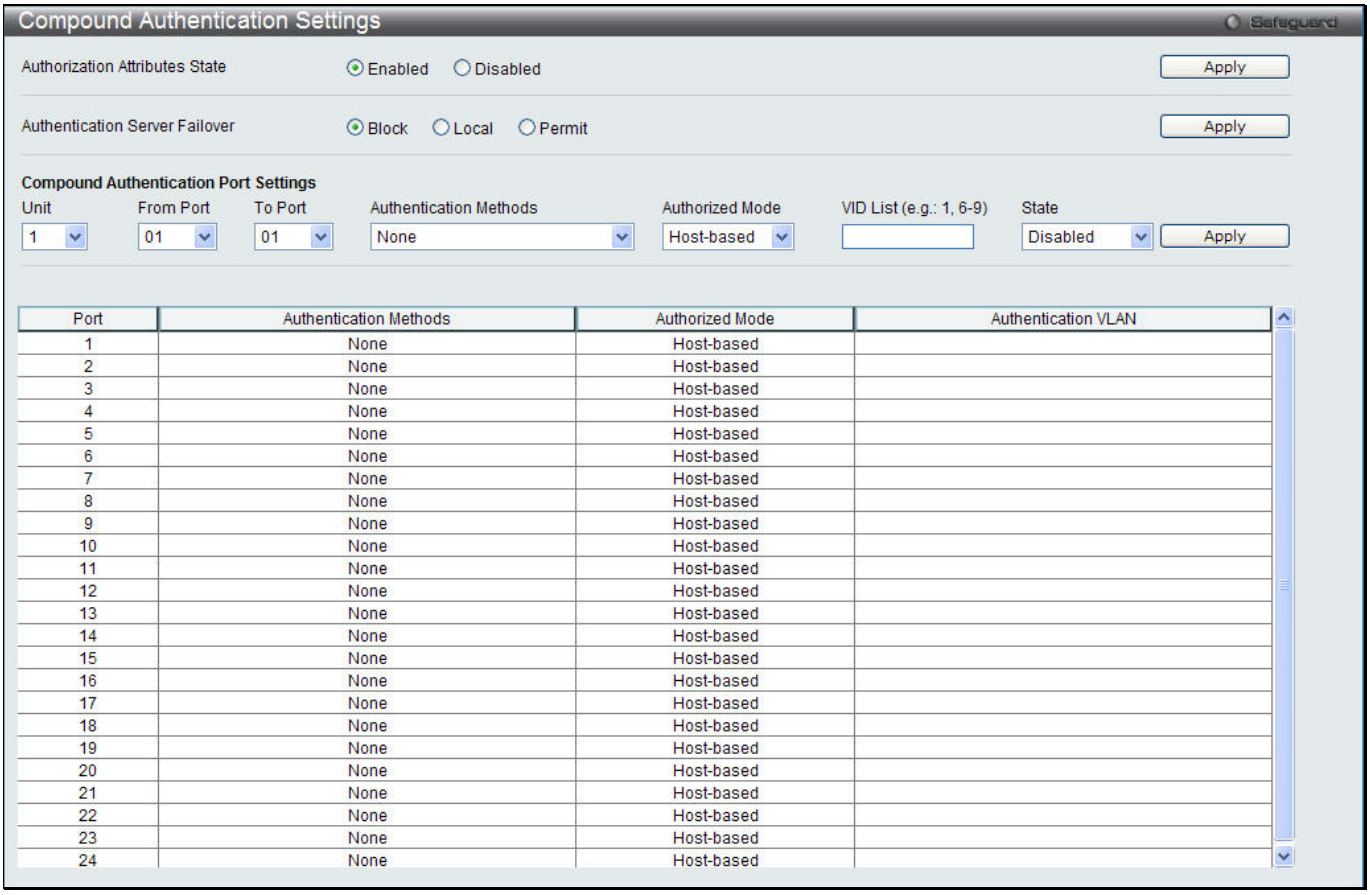
Authentication Server Failover ● Block ○ Local ○ Permit

Compound Authentication Port Settings

Unit	From Port	To Port	Authorized Mode	VID List (e.g.: 1, 6-9)	State
1	01	01	Host-based		Disabled

Port	Authorized Mode	Authentication VLAN
1	Host-based	
2	Host-based	
3	Host-based	
4	Host-based	
5	Host-based	
6	Host-based	
7	Host-based	
8	Host-based	
9	Host-based	
10	Host-based	
11	Host-based	
12	Host-based	
13	Host-based	
14	Host-based	
15	Host-based	
16	Host-based	
17	Host-based	
18	Host-based	
19	Host-based	
20	Host-based	
21	Host-based	
22	Host-based	
23	Host-based	
24	Host-based	

Figure 8-52 Compound Authentication Settings window (SI Mode Only)



Authorization Attributes State ● Enabled ○ Disabled

Authentication Server Failover ● Block ○ Local ○ Permit

Compound Authentication Port Settings

Unit	From Port	To Port	Authentication Methods	Authorized Mode	VID List (e.g.: 1, 6-9)	State
1	01	01	None	Host-based		Disabled

Port	Authentication Methods	Authorized Mode	Authentication VLAN
1	None	Host-based	
2	None	Host-based	
3	None	Host-based	
4	None	Host-based	
5	None	Host-based	
6	None	Host-based	
7	None	Host-based	
8	None	Host-based	
9	None	Host-based	
10	None	Host-based	
11	None	Host-based	
12	None	Host-based	
13	None	Host-based	
14	None	Host-based	
15	None	Host-based	
16	None	Host-based	
17	None	Host-based	
18	None	Host-based	
19	None	Host-based	
20	None	Host-based	
21	None	Host-based	
22	None	Host-based	
23	None	Host-based	
24	None	Host-based	

Figure 8-53 Compound Authentication Settings window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description
Authorization Network State	Click the radio buttons to enable of disable the Authorization Network State.
Authentication Server Failover	Click the radio buttons to configure the authentication server failover function. **Local**. The switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated. **Permit**. The client is always regarded as authenticated. If guest VLAN is enabled, clients will stay on the guest VLAN, otherwise, they will stay on the original VLAN. **Block** (default setting). The client is always regarded as un-authenticated.
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be enabled as compound authentication ports.
Authentication Methods (EI Mode Only)	The compound authentication method options include: None, Any (MAC, 802.1X, JWAC or WAC), 802.1X+IMPB IMPB+JWAC, IMPB+WAC, and MAC+IMPB. *None* - all compound authentication methods are disabled. *Any (MAC, 802.1X, JWAC or WAC)* - if any of the authentication methods pass, then access will be granted. In this mode, MAC, 802.1X, JWAC and WAC can be enabled on a port at the same time. In Any (MAC, 802.1X, JWAC or WAC) mode, whether an individual security module is active on a port depends on its system state. *802.1X+IMPB* - 802.1X will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *IMPB+JWAC* - JWAC will be verified first, and then IMPB will be verified. Both

	authentication methods need to be passed. *IMPB+WAC* - WAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. *MAC+IMPB* - MAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed.
Authorized Mode	Toggle between *Host-based* and *Port-based*. When *Port-based* is selected, if one of the attached hosts passes the authentication, all hosts on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying the next authentication method. When *Host-based* is selected, users are authenticated individually.
VID List	Enter a list of VLAN ID.
State	Use the drop-down menu to assign or remove the specified VID list as authentication VLAN(s).

Click the **Apply** button to accept the changes made for each individual section.

Compound Authentication Guest VLAN Settings (EI Mode Only)

Users can assign ports to or remove ports from a guest VLAN.

To view this window, click **Security > Compound Authentication > Compound Authentication Guest VLAN Settings** as shown below:

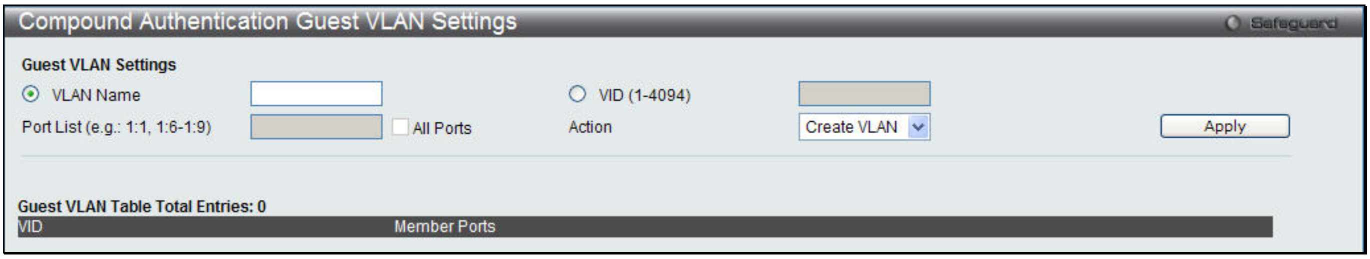

Compound Authentication Guest VLAN Settings
Safeguard
Guest VLAN Settings
● VLAN Name
○ VID (1-4094)
Port List (e.g.: 1:1, 1:6-1:9)
☐ All Ports
Action
Create VLAN
Apply
Guest VLAN Table Total Entries: 0
VID
Member Ports

Figure 8-54 Compound Authentication Guest VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the button and assign a VLAN as a Guest VLAN. The VLAN must be an existing static VLAN.
VID (1-4094)	Click the button and assign a VLAN ID for a Guest VLAN. The VLAN must be an existing static VLAN before this VID can be configured.
Port List	The list of ports to be configured. Alternatively, tick the **All Ports** check box to set every port at once.
Action	Use the drop-down menu to choose the desired operation: *Create VLAN*, *Add Ports*, or *Delete Ports*.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

Once properly configured, the Guest VLAN and associated ports will be listed in the lower part of the window.

IGMP Access Control Settings

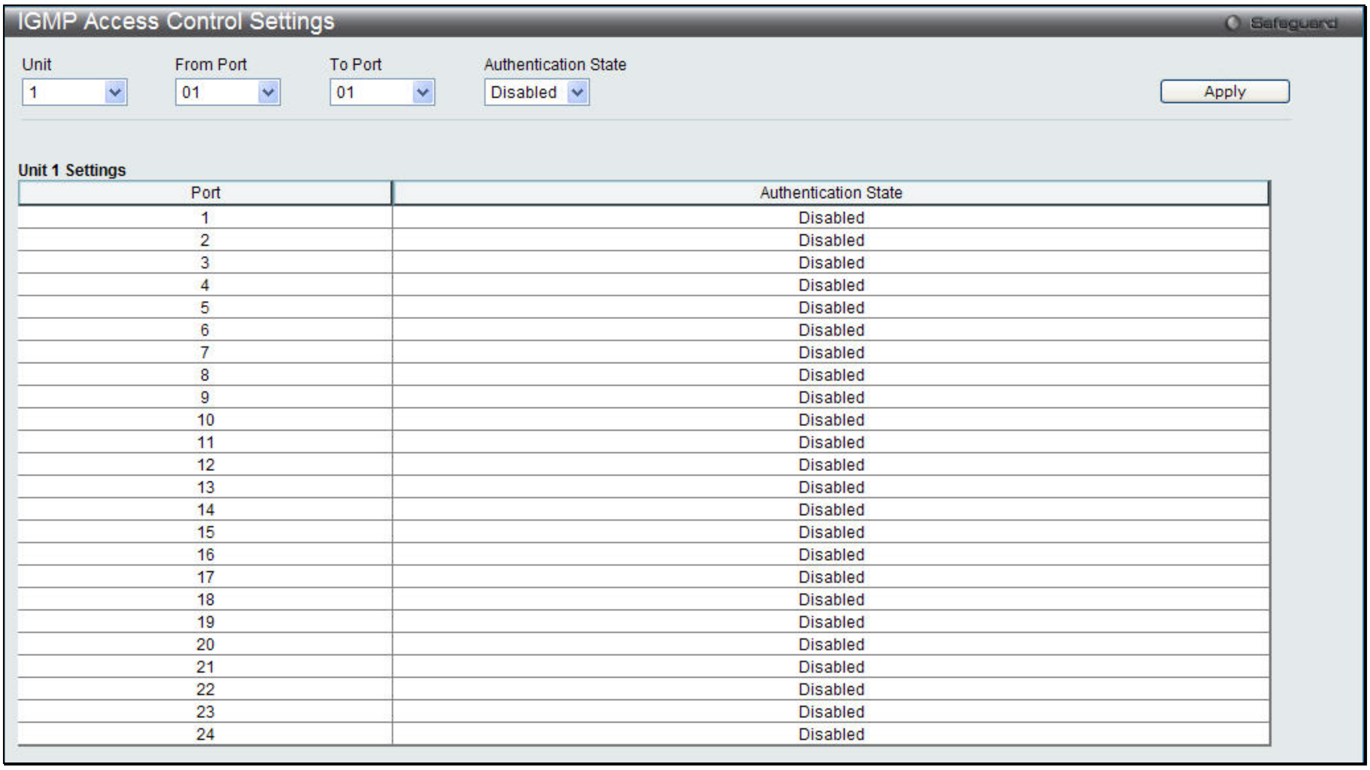
Users can set IGMP authentication, otherwise known as IGMP access control, on individual ports on the Switch. When the **Authentication State** is **Enabled**, and the Switch receives an IGMP join request, the Switch will send the access request to the RADIUS server to do the authentication.

IGMP authentication processes IGMP reports as follows: When a host sends a join message for the interested multicast group, the Switch has to do authentication before learning the multicast group/port. The Switch sends an

Access-Request to an authentication server and the information including host MAC, switch port number, switch IP, and multicast group IP. When the Access-Accept is answered from the authentication server, the Switch learns the multicast group/port. When the Access-Reject is answered from the authentication server, the Switch won't learn the multicast group/port and won't process the packet further. The entry (host MAC, switch port number, and multicast group IP) is put in the "authentication failed list." When there is no answer from the authentication server after T1 time, the Switch resends the Access-Request to the server. If the Switch doesn't receive a response after N1 times, the result is denied and the entry (host MAC, switch port number, multicast group IP) is put in the "authentication failed list." In general case, when the multicast group/port is already learned by the switch, it won't do the authentication again. It only processes the packet as standard.

IGMP authentication processes IGMP leaves as follows: When the host sends leave message for the specific multicast group, the Switch follows the standard procedure for leaving a group and then sends an Accounting-Request to the accounting server for notification. If there is no answer from the accounting server after T2 time, the Switch resends the Accounting-Request to the server. The maximum number of retry times is N2.

To view this window, click **Security > IGMP Access Control Settings** as shown below:



Unit: 1
From Port: 01
To Port: 01
Authentication State: Disabled

Unit 1 Settings

Port	Authentication State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be enabled as compound authentication ports.
Authentication State	Use the drop-down menu to enable or disable the authentication state.

Click the **Apply** button to accept the changes made.

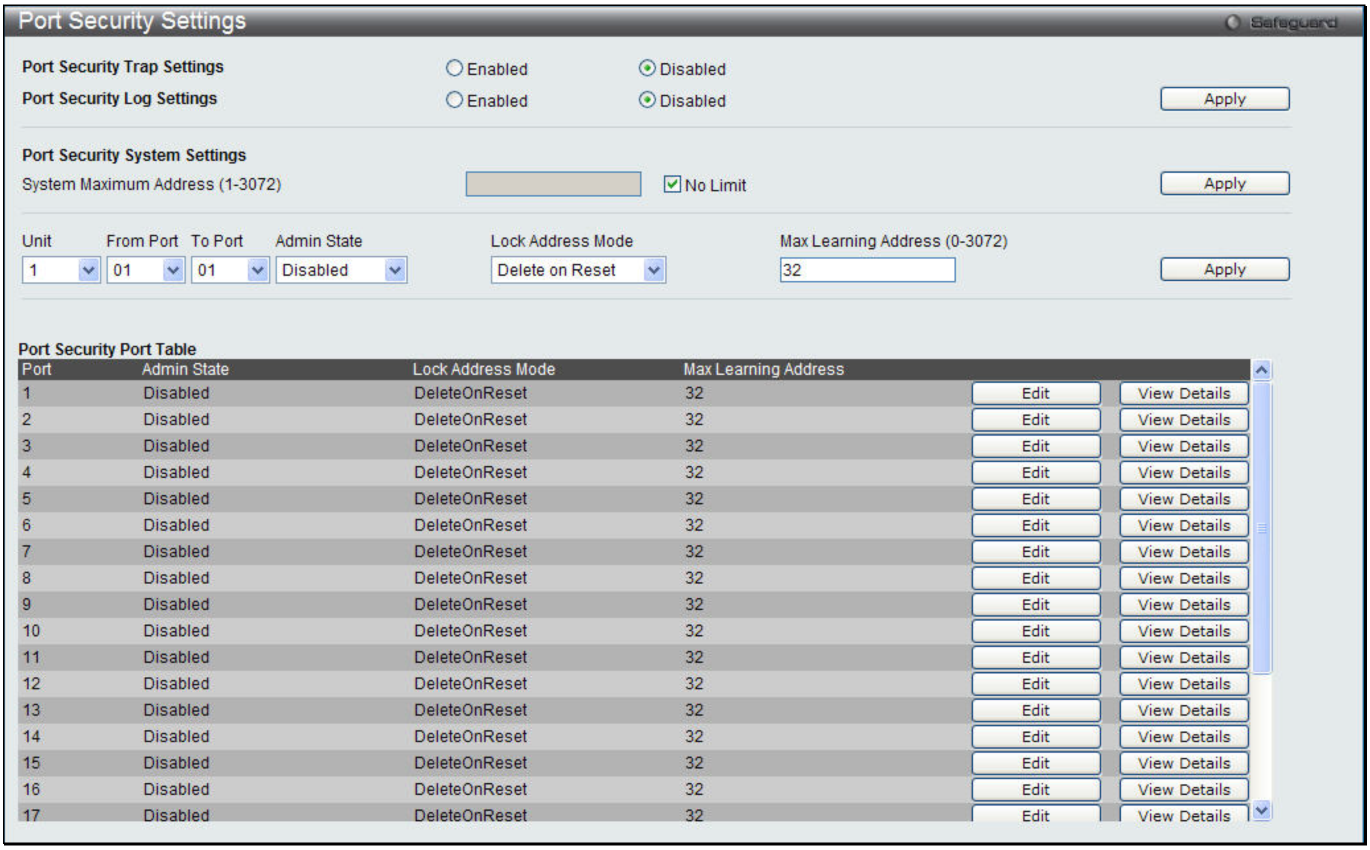
Port Security

Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled. The port can be locked by changing the **Admin State** drop-down menu to *Enabled* and clicking **Apply**.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view this window, click **Security > Port Security > Port Security Settings** as shown below:



Port Security Trap Settings ○ Enabled ● Disabled

Port Security Log Settings ○ Enabled ● Disabled

Port Security System Settings

System Maximum Address (1-3072) ☑ No Limit

Unit	From Port	To Port	Admin State	Lock Address Mode	Max Learning Address (0-3072)
1	01	01	Disabled	Delete on Reset	32

Port Security Port Table

Port	Admin State	Lock Address Mode	Max Learning Address		
1	Disabled	DeleteOnReset	32	Edit	View Details
2	Disabled	DeleteOnReset	32	Edit	View Details
3	Disabled	DeleteOnReset	32	Edit	View Details
4	Disabled	DeleteOnReset	32	Edit	View Details
5	Disabled	DeleteOnReset	32	Edit	View Details
6	Disabled	DeleteOnReset	32	Edit	View Details
7	Disabled	DeleteOnReset	32	Edit	View Details
8	Disabled	DeleteOnReset	32	Edit	View Details
9	Disabled	DeleteOnReset	32	Edit	View Details
10	Disabled	DeleteOnReset	32	Edit	View Details
11	Disabled	DeleteOnReset	32	Edit	View Details
12	Disabled	DeleteOnReset	32	Edit	View Details
13	Disabled	DeleteOnReset	32	Edit	View Details
14	Disabled	DeleteOnReset	32	Edit	View Details
15	Disabled	DeleteOnReset	32	Edit	View Details
16	Disabled	DeleteOnReset	32	Edit	View Details
17	Disabled	DeleteOnReset	32	Edit	View Details

Figure 8-55 Port Security Settings window

The fields that can be configured are described below:

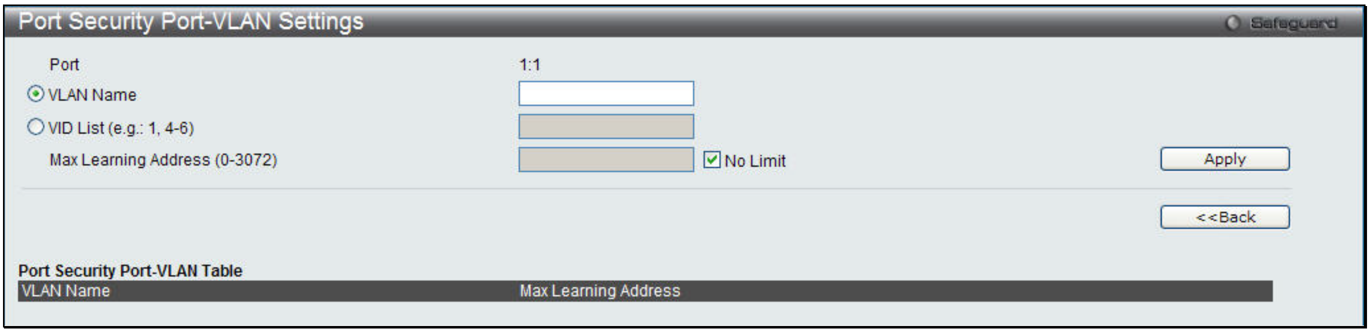
Parameter	Description
Port Security Trap Settings	Click to enable or disable Port Security Traps on the Switch.
Port Security Log Settings	Click to enable or disable Port Security Logs on the Switch.
System Max Address (1-3072)	Enter the system maximum address. Tick the **No Limit** check box to have unlimited system addresses.
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured.
Admin State	Use the drop-down menu to enable or disable Port Security (locked MAC address table for the selected ports).
Lock Address Mode	This drop-down menu allows the option of how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: *Permanent* – The locked addresses will only age out after the Switch has been reset. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been reset or rebooted.
Max Learning Address (0-3072)	Specify the maximum value of port security entries that can be learned on this port.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Edit** button to re-configure the specific entry.

Click the **View Detail** button to display the information of the specific entry.

After clicking the **View Detail** button, the following page will appear:



Port Security Port-VLAN Settings

Port 1:1

● VLAN Name

○ VID List (e.g.: 1, 4-6)

Max Learning Address (0-3072) ☑ No Limit

Port Security Port-VLAN Table

VLAN Name	Max Learning Address

Figure 8-56 Port Security Port-VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VLAN Name	Click the button and enter the name of the VLAN that the port security settings will be displayed for.
VID List	Click the button and enter VLAN IDs that the port security settings will be displayed for.
Max Learning Address (0-3072)	Specify the maximum value of port security entries that can be learned on this port. Tick the **No Limit** check box to have unlimited number of port security entries that can be learned by the system.

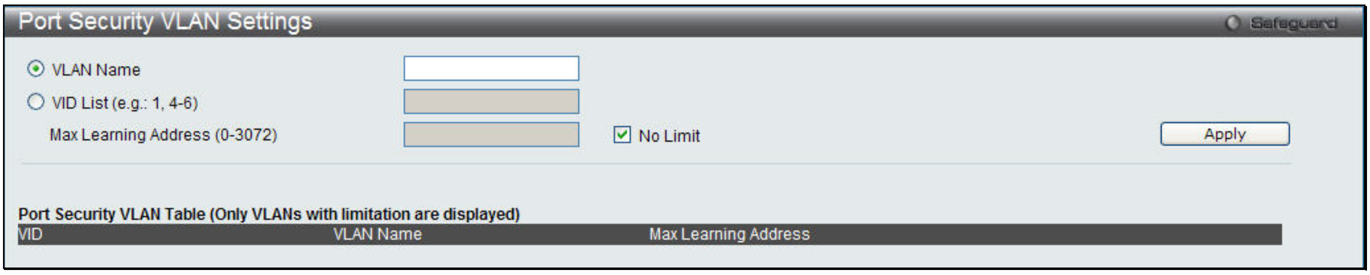
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Port Security VLAN Settings

Users can configure the maximum number of port-security entries that can be learned on a specific VLAN.

To view this window, click **Security > Port Security > Port Security VLAN Settings** as shown below:



Port Security VLAN Settings

● VLAN Name

○ VID List (e.g.: 1, 4-6)

Max Learning Address (0-3072) ☑ No Limit

Port Security VLAN Table (Only VLANs with limitation are displayed)

VID	VLAN Name	Max Learning Address

Figure 8-57 Port Security VLAN Settings window

The fields that can be configured are described below:

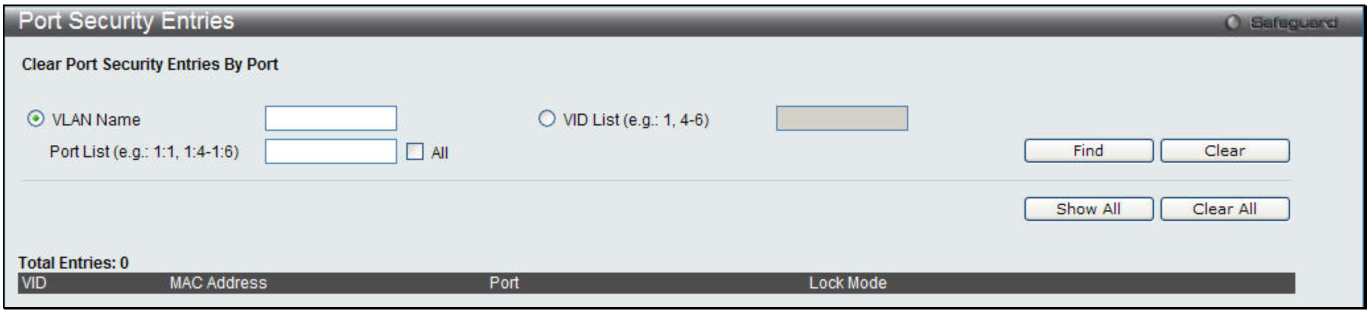
Parameter	Description
VLAN Name	Enter the VLAN Name.
VID List	Specify a list of the VLAN be VLAN ID.
Max Learning Address	Specify the maximum number of port-security entries that can be learned by this VLAN. Tick the **No Limit** check box to have unlimited number of port security entries that can be learned by the VLAN.

Click the **Apply** button to accept the changes made.

Port Security Entries

Users can remove an entry from the port security entries learned by the Switch and entered into the forwarding database.

To view this window, click **Security > Port Security > Port Security Entries** as shown below:


Port Security Entries
Safeguard
Clear Port Security Entries By Port
● VLAN Name
○ VID List (e.g.: 1, 4-6)
Port List (e.g.: 1:1, 1:4-1:6)
☐ All
Find
Clear
Show All
Clear All

Total Entries: 0

VID	MAC Address	Port	Lock Mode

Figure 8-58 Port Security Entries window

The fields that can be configured or displayed are described below:

Parameter	Description
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
VID List	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
Port List	Enter the port number or list here to be used for the port security entry search. When **All** is selected, all the ports configured will be displayed.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Lock Mode	The type of MAC address in the forwarding database table.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the entries based on the information entered.

Click the **Show All** button to display all the existing entries.

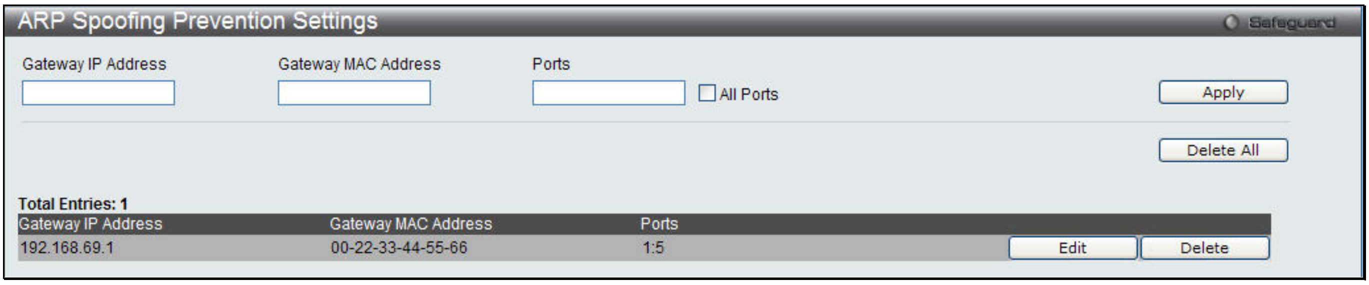
Click the **Clear All** button to remove all the entries listed.

Click the **Delete** button to remove the specific entry.

ARP Spoofing Prevention Settings

The user can configure the spoofing prevention entry to prevent spoofing of MAC for the protected gateway. When an entry is created, those ARP packets whose sender IP matches the gateway IP of an entry, but either its sender MAC field or source MAC field does not match the gateway MAC of the entry will be dropped by the system.

To view this window, click **Security > ARP Spoofing Prevention Settings** as shown below:


ARP Spoofing Prevention Settings
Safeguard
Gateway IP Address
Gateway MAC Address
Ports
☐ All Ports
Apply
Delete All
Edit
Delete

Total Entries: 1

Gateway IP Address	Gateway MAC Address	Ports
192.168.69.1	00-22-33-44-55-66	1:5

Figure 8-59 ARP Spoofing Prevention Settings window

The fields that can be configured are described below:

Parameter	Description
Gateway IP Address	Enter the gateway IP address to help prevent ARP Spoofing.
Gateway MAC Address	Enter the gateway MAC address to help prevent ARP Spoofing.
Ports	Enter the port numbers that this feature applies to. Alternatively the user can select **All Ports** to apply this feature to all the ports of the switch.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

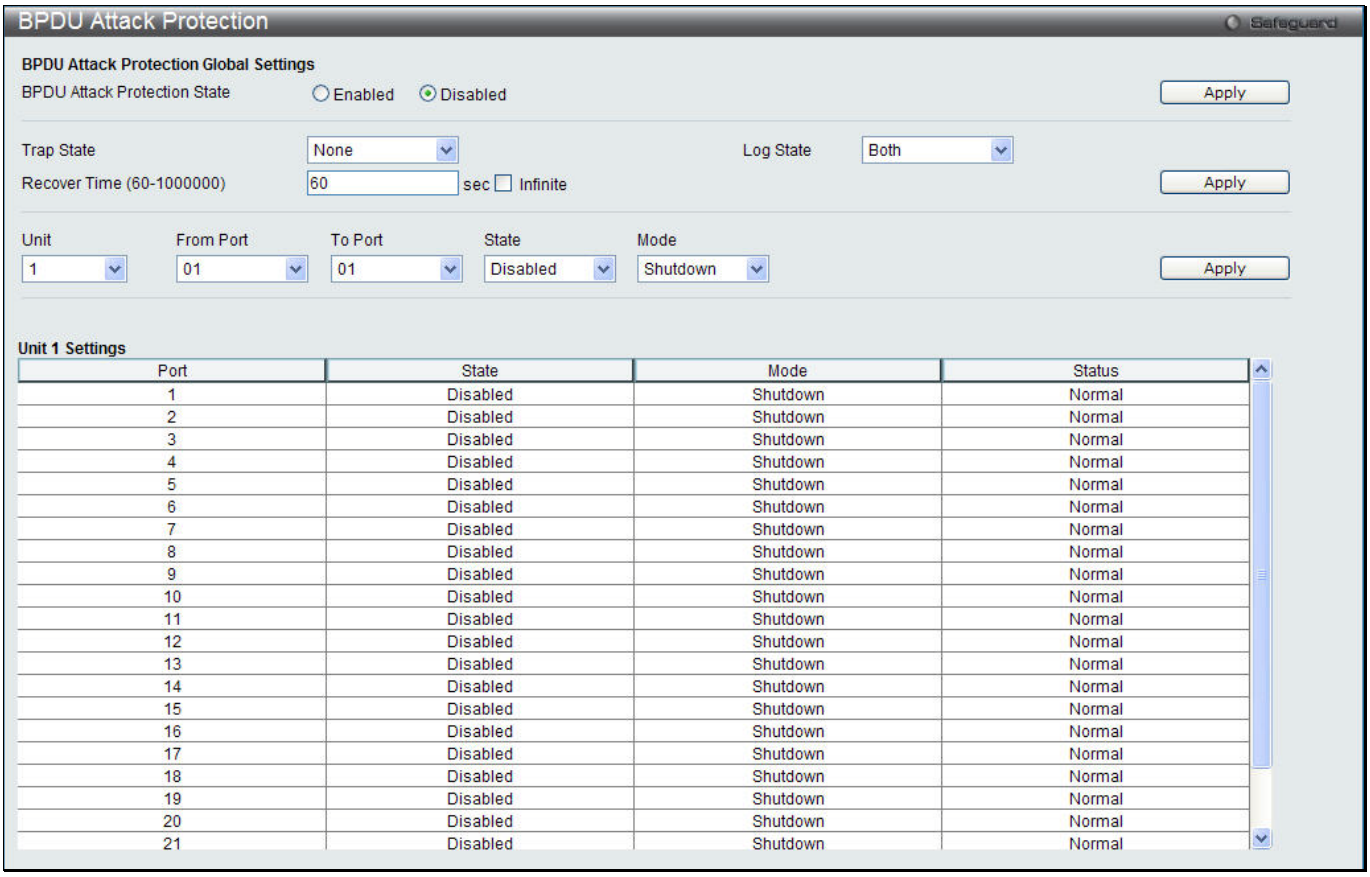
BPDU Attack Protection

This page is used to configure the BPDU protection function for the ports on the switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter an under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port.

BPDU protection has a higher priority than the FBPDU setting configured by configure STP command in the determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has a higher priority than the BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view this window, click **Security > BPDU Attack Protection** as shown below:



BPDU Attack Protection Global Settings

BPDU Attack Protection State ○ Enabled ● Disabled

Trap State: None

Log State: Both

Recover Time (60-1000000): 60 sec ☐ Infinite

Unit: 1

From Port: 01

To Port: 01

State: Disabled

Mode: Shutdown

Unit 1 Settings

Port	State	Mode	Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal
11	Disabled	Shutdown	Normal
12	Disabled	Shutdown	Normal
13	Disabled	Shutdown	Normal
14	Disabled	Shutdown	Normal
15	Disabled	Shutdown	Normal
16	Disabled	Shutdown	Normal
17	Disabled	Shutdown	Normal
18	Disabled	Shutdown	Normal
19	Disabled	Shutdown	Normal
20	Disabled	Shutdown	Normal
21	Disabled	Shutdown	Normal

Figure 8-60 BPDU Attack Protection window

The fields that can be configured are described below:

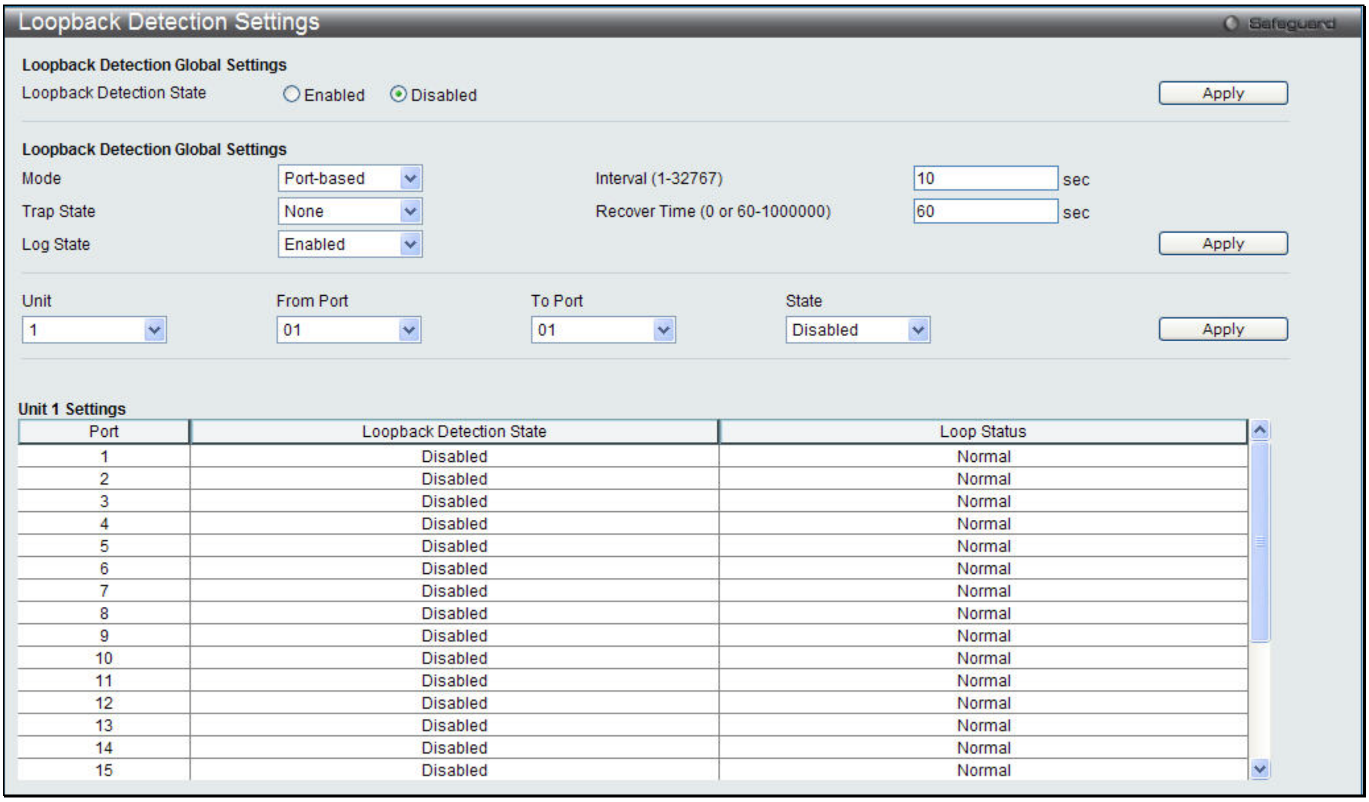
Parameter	Description
BPDU Attack Protection State	Click the radio buttons to enable or disable the BPDU Attack Protection state.
Trap State	Specify when a trap will be sent. Options to choose from are **None**, **Attack Detected**, **Attack Cleared** or **Both**.
Log State	Specify when a log entry will be sent. Options to choose from are **None**, **Attack Detected**, **Attack Cleared** or **Both**.
Recover Time (60-1000000)	Specify the BPDU protection Auto-Recovery timer. The default value of the recovery timer is *60*.
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports to use for this configuration.
State	Use the drop-down menu to enable or disable the protection mode for a specific port.
Mode	Specify the BPDU protection mode. The default mode is shutdown. *Drop* – Drop all received BPDU packets when the port enters under attack state. *Block* – Drop all packets (include BPDU and normal packets) when the port enters under attack state. *Shutdown* – Shut down the port when the port enters under attack state.

Click the **Apply** button to accept the changes made for each individual section.

Loopback Detection Settings

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port or a VLAN, this signifies a loop on the network. The Switch will automatically block the port or the VLAN and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view this window, click **Security > Loopback Detection Settings** as shown below:



Loopback Detection Global Settings

Loopback Detection State ○ Enabled ● Disabled

Loopback Detection Global Settings

Mode: Port-based
Trap State: None
Log State: Enabled
Interval (1-32767): 10 sec
Recover Time (0 or 60-1000000): 60 sec

Unit: 1
From Port: 01
To Port: 01
State: Disabled

Unit 1 Settings

Port	Loopback Detection State	Loop Status
1	Disabled	Normal
2	Disabled	Normal
3	Disabled	Normal
4	Disabled	Normal
5	Disabled	Normal
6	Disabled	Normal
7	Disabled	Normal
8	Disabled	Normal
9	Disabled	Normal
10	Disabled	Normal
11	Disabled	Normal
12	Disabled	Normal
13	Disabled	Normal
14	Disabled	Normal
15	Disabled	Normal

Figure 8-61 Loopback Detection Settings window

The fields that can be configured are described below:

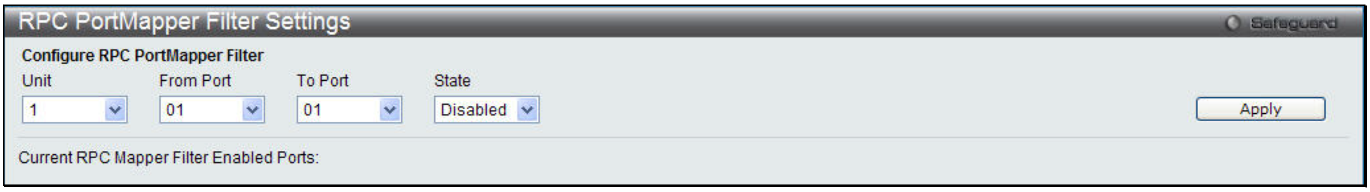
Parameter	Description
Loopback Detection State	Use the radio button to enable or disable loopback detection. The default is Disabled.
Mode	Use the drop-down menu to toggle between *Port-based* and *VLAN-based*.
Trap State	Set the desired trap status: *None*, *Loop Detected*, *Loop Cleared*, or *Both*.
Log State	Specifies the state of the log for loopback detection.
Interval (1-32767)	The time interval (in seconds) that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The valid range is from *1* to *32767* seconds. The default setting is *10* seconds.
Recover Time (0 or 60-1000000)	Time allowed (in seconds) for recovery when a Loopback is detected. The Loop-detect Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop-detect Recover Time. The default is *60* seconds.
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured.
State	Use the drop-down menu to toggle between *Enabled* and *Disabled*.

Click the **Apply** button to accept the changes made for each individual section.

RPC PortMapper Filter Settings

This window is used to configure and display the RPC portmapper filter state on the specific ports. The RPC portmapper service listens on a static port (TCP or UDP port 135). It converts the RPC program numbers into TCP/IP (or UDP/IP) protocol port numbers. Some Microsoft applications and services such as Outlook, Exchange, and the Messenger Service also use this service and listen on both TCP and UDP port 135 for endpoint mapping. For management and security concerns, the purpose of this feature is to filter the TCP/UDP port 135 for prohibition of some unwanted services.

To view this window, click **Security > RPC PortMapper Filter Settings** as shown below:



RPC PortMapper Filter Settings

Configure RPC PortMapper Filter

Unit	From Port	To Port	State
1	01	01	Disabled

Current RPC Mapper Filter Enabled Ports:

Figure 8-62 RPC Port Mapper Filter Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured.
State	Use the drop-down menu to enable or disable RPC portmapper filter on specified ports.

Click the **Apply** button to accept the changes made.

NetBIOS Filtering Settings

NetBIOS is an application programming interface, providing a set of functions that applications use to communicate across networks. NetBEUI, the NetBIOS Enhanced User Interface, was created as a data-link-layer frame structure for NetBIOS. A simple mechanism to carry NetBIOS traffic, NetBEUI has been the protocol of choice for small MS-DOS- and Windows-based workgroups. NetBIOS no longer lives strictly inside of the NetBEUI protocol. Microsoft worked to create the international standards described in RFC 1001 and RFC 1002, NetBIOS over TCP/IP (NBT).

If the network administrator wants to block the network communication on more than two computers which use NETBUEI protocol, it can use NETBIOS filtering to filter these kinds of packets.

If the user enables the NETBIOS filter, the switch will create one access profile and three access rules automatically. If the user enables the extensive NETBIOS filter, the switch will create one more access profile and one more access rule.

To view this window, click **Security > NetBIOS Filtering Settings** as shown below:

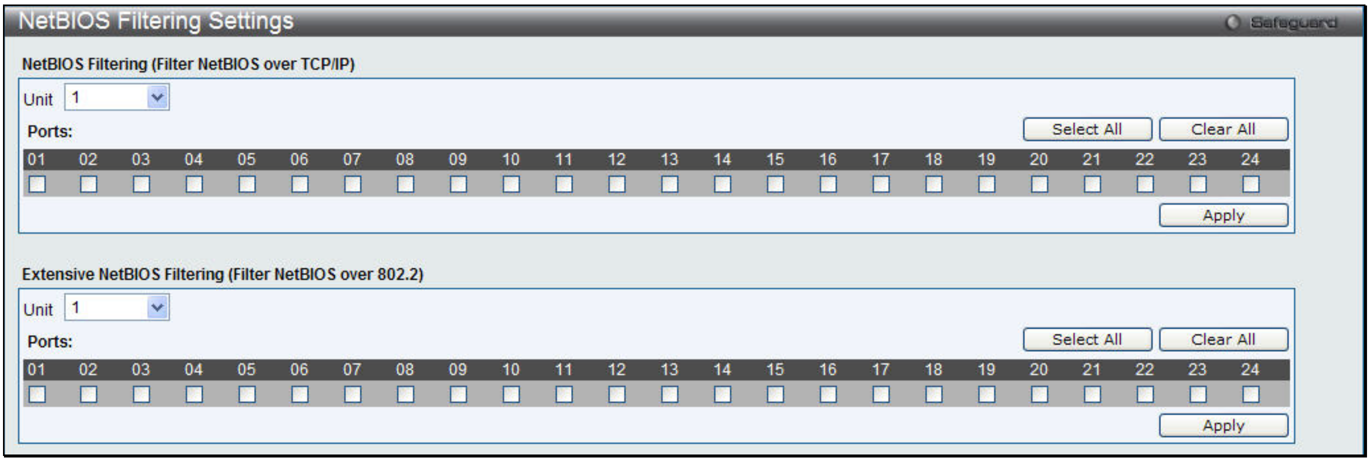

NetBIOS Filtering Settings
Safeguard
NetBIOS Filtering (Filter NetBIOS over TCP/IP)
Unit 1
Ports:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Apply
Extensive NetBIOS Filtering (Filter NetBIOS over 802.2)
Unit 1
Ports:
Select All
Clear All
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Apply

Figure 8-63 NetBIOS Filtering Settings window

The fields that can be configured are described below:

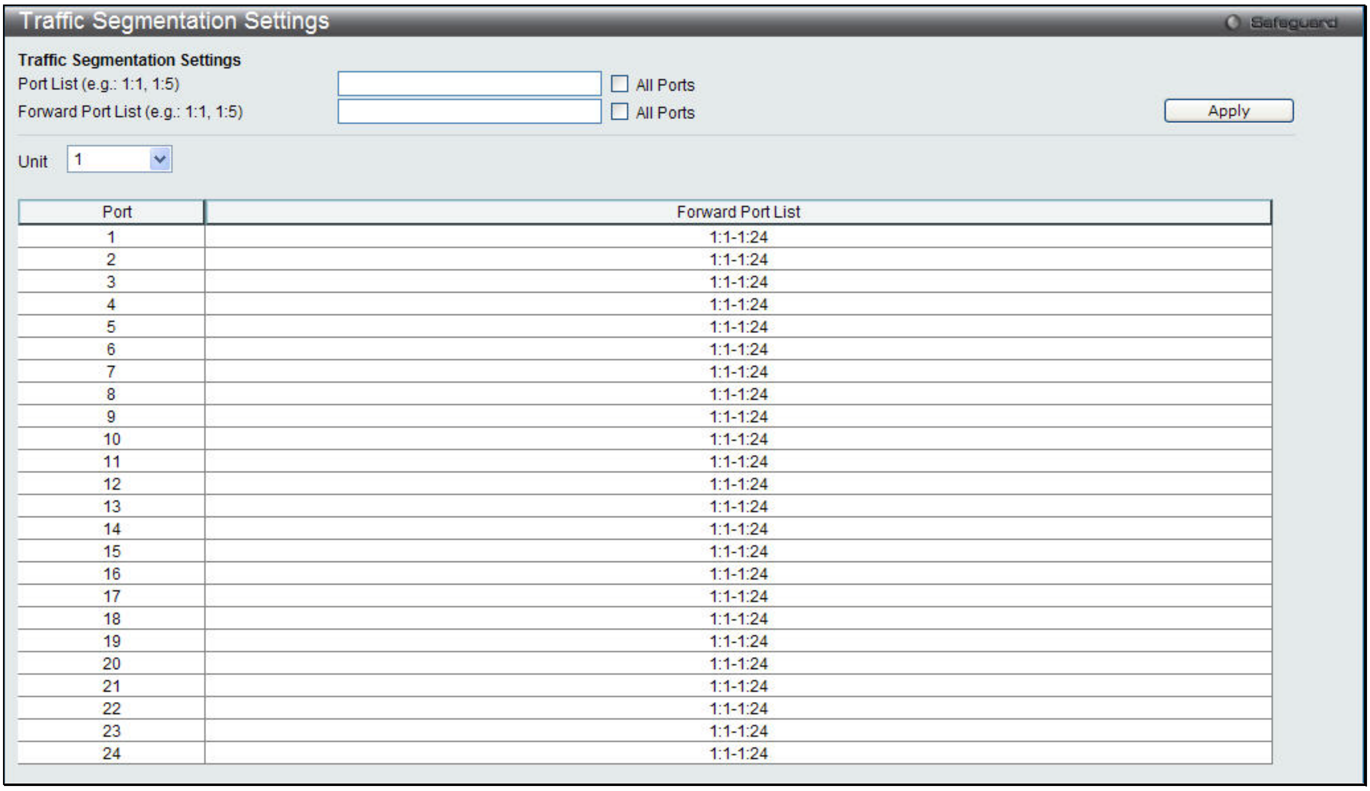
Parameter	Description
NetBIOS Filtering Ports	Select the appropriate port to include in the NetBIOS filtering configuration.
Extensive NetBIOS Filtering Ports	Select the appropriate port to include in the Extensive NetBIOS filtering configuration. Extensive NetBIOS is NetBIOS over 802.3. The Switch will deny the NetBIOS over 802.3 frame on these enabled ports.
Unit	Select the unit you want to configure.
Ports	Tick the appropriate ports to be configured. Click the **Select All** button to select all ports. Click the **Clear All** button to deselect all ports.

Click the **Apply** button to accept the changes made for each individual section.

Traffic Segmentation Settings

Traffic segmentation is used to limit traffic flow from a single or group of ports, to a group of ports. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the master switch CPU.

To view this window, click **Security > Traffic Segmentation Settings** as shown below:



Traffic Segmentation Settings

Port List (e.g.: 1:1, 1:5) ☐ All Ports

Forward Port List (e.g.: 1:1, 1:5) ☐ All Ports

Unit 1

Port	Forward Port List
1	1:1-1:24
2	1:1-1:24
3	1:1-1:24
4	1:1-1:24
5	1:1-1:24
6	1:1-1:24
7	1:1-1:24
8	1:1-1:24
9	1:1-1:24
10	1:1-1:24
11	1:1-1:24
12	1:1-1:24
13	1:1-1:24
14	1:1-1:24
15	1:1-1:24
16	1:1-1:24
17	1:1-1:24
18	1:1-1:24
19	1:1-1:24
20	1:1-1:24
21	1:1-1:24
22	1:1-1:24
23	1:1-1:24
24	1:1-1:24

Figure 8-64 Traffic Segmentation Settings window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter a list of ports to be included in the traffic segmentation setup. Tick the **All ports** check box to select all ports.
Forward Port List	Enter a list of ports to be included in the traffic segmentation setup. by simply ticking the corresponding port’s tick box. Tick the **All ports** check box to select all ports.
Unit	Select the unit you want to configure.

Click the **Apply** button to accept the changes made.

DHCP Server Screening

This function allows the user to not only to restrict all DHCP Server packets but also to receive any specified DHCP server packet by any specified DHCP client, it is useful when one or more DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients.

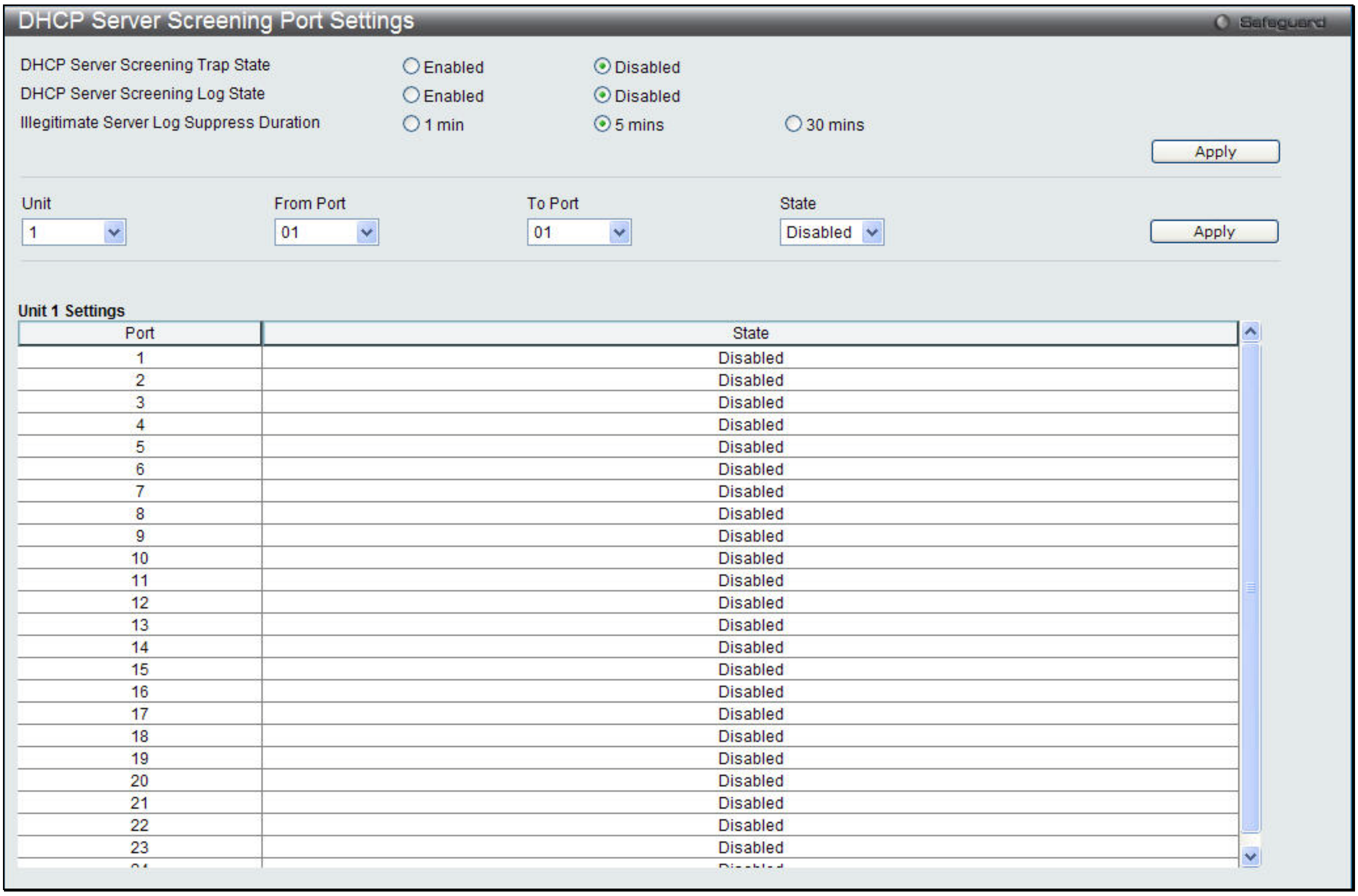
The first time the DHCP filter is enabled it will create both an access profile entry and an access rule per port entry, it will also create other access rules. These rules are used to block all DHCP server packets. In addition to a permit DHCP entry it will also create one access profile and one access rule entry the first time the DHCP client MAC address is used as the client MAC address. The Source IP address is the same as the DHCP server’s IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fields, which the user has configured.

When DHCP Server filter function is enabled all DHCP Server packets will be filtered from a specific port.

DHCP Server Screening Port Settings

The Switch supports DHCP Server Screening, a feature that denies access to rogue DHCP servers. When the DHCP server filter function is enabled, all DHCP server packets will be filtered from a specific port.

To view this window, click **Security > DHCP Server Screening > DHCP Server Screening Port Settings** as shown below:



DHCP Server Screening Trap State ○ Enabled ● Disabled

DHCP Server Screening Log State ○ Enabled ● Disabled

Illegitimate Server Log Suppress Duration ○ 1 min ● 5 mins ○ 30 mins

Unit	From Port	To Port	State
1	01	01	Disabled

Unit 1 Settings

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled

Figure 8-65 DHCP Server Screening Port Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Server Trap State	Click to enable or disable filtering DHCP server trap.
DHCP Server Log State	Click to enable or disable filtering DHCP server log.
Illegal Server Log Suppress Duration	Choose an illegal server log suppress duration of 1 minute, 5 minutes, or 30 minutes.
Unit	Select the unit you want to configure.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured.
State	Choose *Enabled* to enable the DHCP server screening or *Disabled* to disable it. The default is *Disabled*.

Click the **Apply** button to accept the changes made for each individual section.

DHCP Offer Permit Entry Settings

Users can add or delete permit entries on this page.

To view this window, click **Security > DHCP Server Screening > DHCP Offer Permit Entry Settings** as shown below:

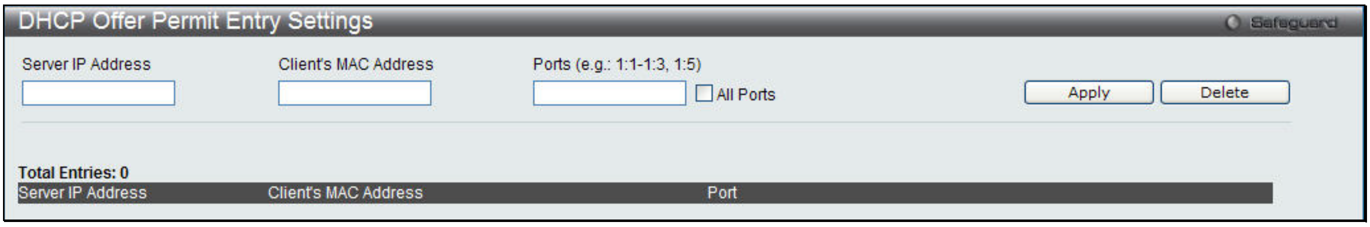


Figure 8-66 DHCP Offer Permit Entry Settings window

The fields that can be configured are described below:

Parameter	Description
Server IP Address	The IP address of the DHCP server to be permitted.
Client’s MAC Address	The MAC address of the DHCP client.
Ports	The port numbers of the filter DHCP server. Tick the **All Ports** check box to include all the ports on this switch for this configuration.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry based on the information entered.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- **TACACS+ (Terminal Access Controller Access Control System plus**) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

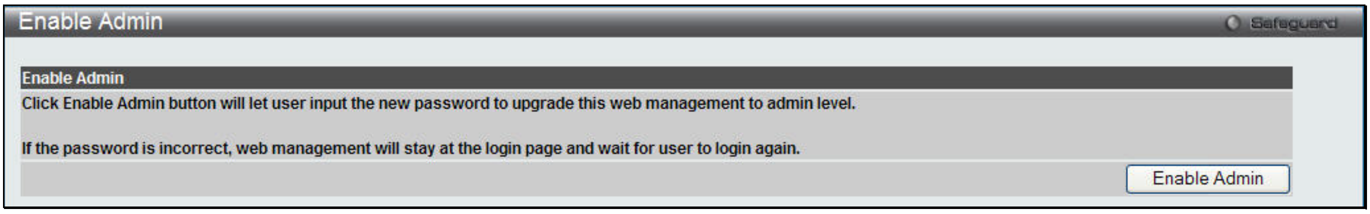
Users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Enable Admin

Users who have logged on to the Switch on the normal user level and wish to be promoted to the administrator level can use this window. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view this window, click **Security > Access Authentication Control > Enable Admin** as shown below:

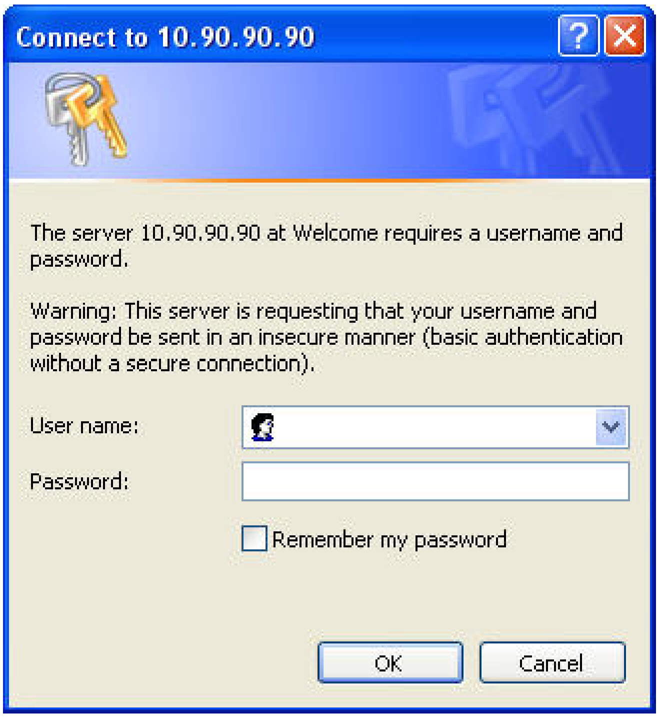


Click Enable Admin button will let user input the new password to upgrade this web management to admin level.

If the password is incorrect, web management will stay at the login page and wait for user to login again.

Figure 8-67 Enable Admin window

When this window appears, click the **Enable Admin** button revealing a window for the user to enter authentication (password, username), as shown below. A successful entry will promote the user to Administrator level privileges on the Switch.



The server 10.90.90.90 at Welcome requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name:

Password:

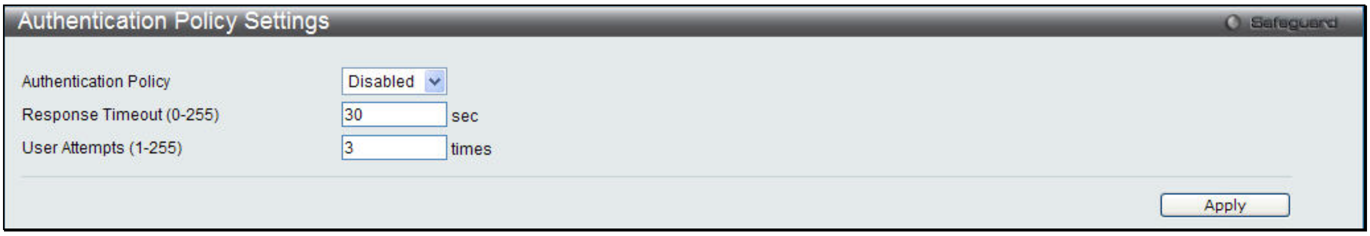
☐ Remember my password

Figure 8-68 Log-in Page

Authentication Policy Settings

Users can enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

To view this window, click **Security > Access Authentication Control > Authentication Policy Settings** as shown below:



Authentication Policy: Disabled

Response Timeout (0-255): 30 sec

User Attempts (1-255): 3 times

Figure 8-69 Authentication Policy Settings window

The fields that can be configured are described below:

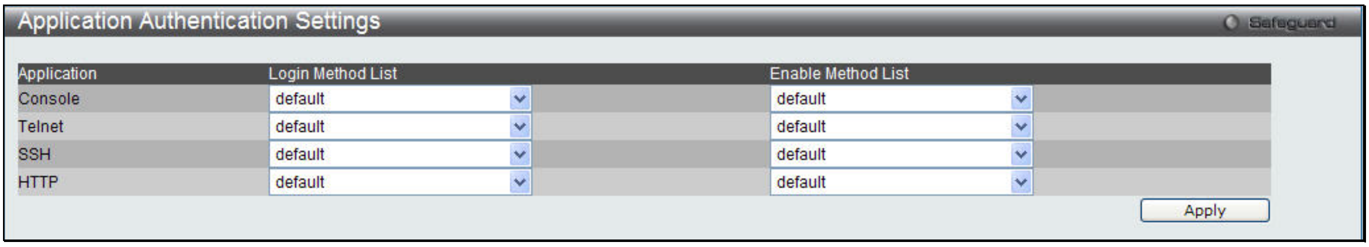
Parameter	Description
Authentication Policy	Use the drop-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click the **Apply** button to accept the changes made.

Application Authentication Settings

Users can configure Switch configuration applications (Console, Telnet, SSH, HTTP) for login at the user level and at the administration level (Enable Admin**)** utilizing a previously configured method list.

To view this window, click **Security > Access Authentication Control > Application Authentication Settings** as shown below:



Application	Login Method List	Enable Method List
Console	default	default
Telnet	default	default
SSH	default	default
HTTP	default	default

Figure 8-70 Application Authentication Settings window

The fields that can be configured are described below:

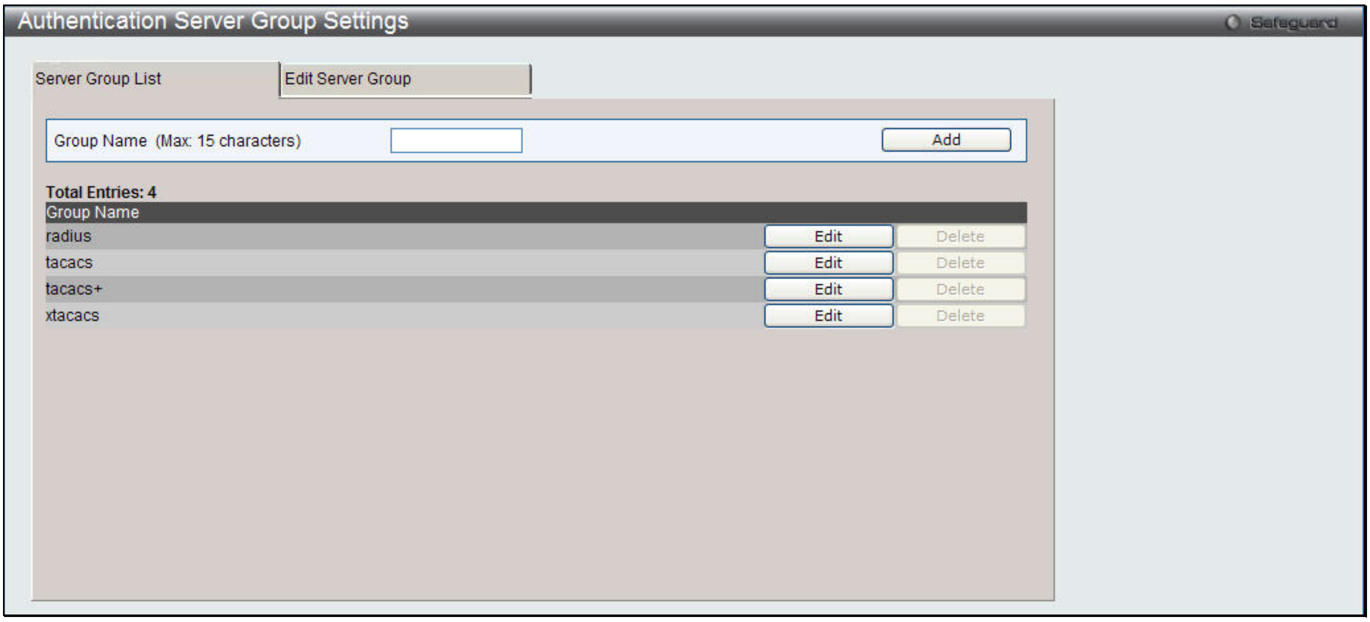
Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH, and the Web (HTTP) application.
Login Method List	Using the drop-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists window, in this section, for more information.
Enable Method List	Using the drop-down menu, configure an application to promote user level to admin-level users utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Enable Method Lists window, in this section, for more information

Click the **Apply** button to accept the changes made.

Authentication Server Group Settings

Users can set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view this window, click **Security > Access Authentication Control > Authentication Server Group Settings** as shown below:


Authentication Server Group Settings
Safeguard
Server Group List
Edit Server Group
Group Name (Max: 15 characters)
Add
Edit
Delete

Total Entries: 4

Group Name
radius
tacacs
tacacs+
xtacacs

Figure 8-71 Authentication Server Group Settings – Server Group List window

This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To add a new Server Group, enter a name in the **Group Name** field and then click the **Add** button. To modify a particular group, click the **Edit** button (or the **Edit Server Group** tab), which will then display the following **Edit Server Group** tab:

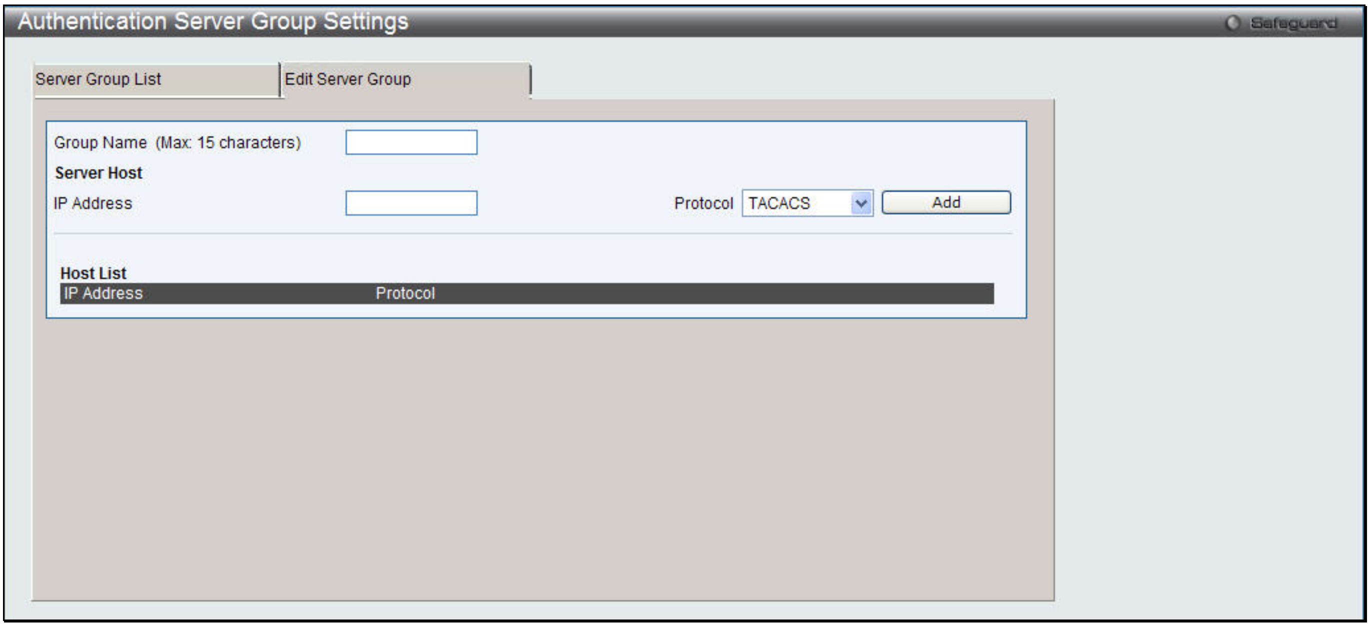

Authentication Server Group Settings
Safeguard
Server Group List
Edit Server Group
Group Name (Max: 15 characters)
Server Host
IP Address
Protocol
TACACS
Add
Host List
IP Address
Protocol

Figure 8-72 Authentication Server Group Settings – Edit Server Group window

To add an Authentication Server Host to the list, enter its name in the **Group Name** field, IP address in the **IP Address** field, use the drop-down menu to choose the **Protocol** associated with the IP address of the Authentication Server Host, and then click **Add** to add this Authentication Server Host to the group. The entry should appear in the Host List at the bottom of this tab.

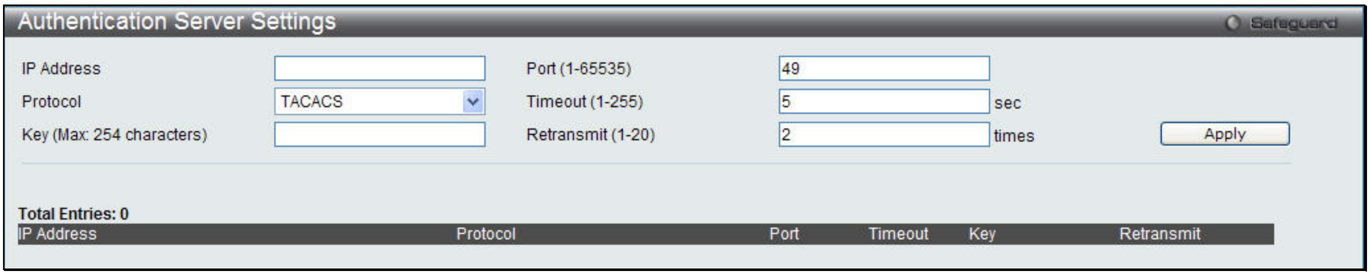
NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE: The three built-in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server Settings

User-defined Authentication Server Hosts for the TACACS / XTACACS / TACACS+ / RADIUS security protocols can be set on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view this window, click **Security > Access Authentication Control > Authentication Server Settings** as shown below:



IP Address:
Protocol: TACACS
Key (Max: 254 characters):
Port (1-65535): 49
Timeout (1-255): 5 sec
Retransmit (1-20): 2 times

Total Entries: 0

IP Address	Protocol	Port	Timeout	Key	Retransmit

Figure 8-73 Authentication Server Settings window

The fields that can be configured are described below:

Parameter	Description
IP Address	The IP address of the remote server host to add.
Protocol	The protocol used by the server host. The user may choose one of the following: *TACACS* - Enter this parameter if the server host utilizes the TACACS protocol. *XTACACS* - Enter this parameter if the server host utilizes the XTACACS protocol. *TACACS+* - Enter this parameter if the server host utilizes the TACACS+ protocol. *RADIUS* - Enter this parameter if the server host utilizes the RADIUS protocol.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.
Port (1-65535)	Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1813* for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.
Retransmit (1-20)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This value will not take effect when configuring to TACACS+. The default value is *2*.

Click the **Apply** button to accept the changes made.

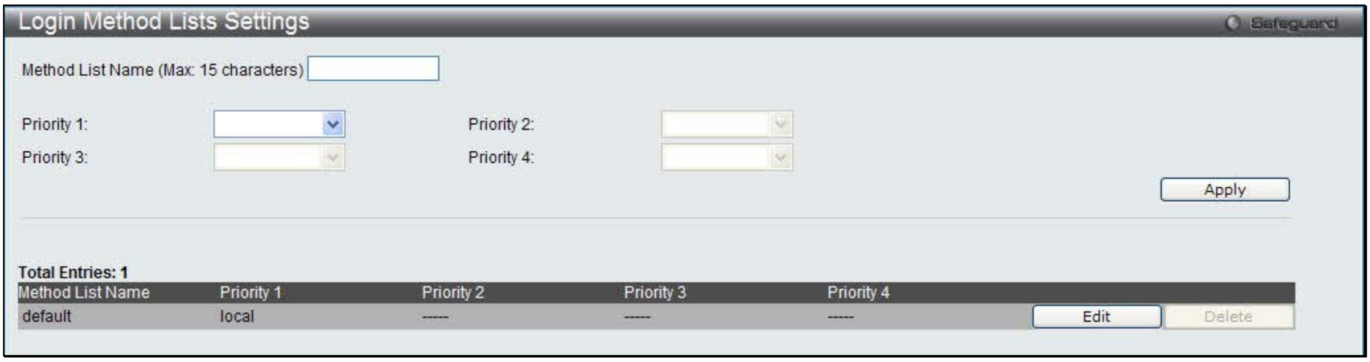
NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

Login Method Lists Settings

User-defined or default Login Method List of authentication techniques can be configured for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependent on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a "User" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator.

To view this window, click **Security > Access Authentication Control > Login Method Lists Settings** as shown below:


Login Method Lists Settings
Safeguard
Method List Name (Max: 15 characters)
Priority 1:
Priority 2:
Priority 3:
Priority 4:
Apply

Total Entries: 1

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4		
default	local	-----	-----	-----	Edit	Delete

Figure 8-74 Login Method Lists Settings window

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the **Delete** button corresponding to the entry desired to be deleted. To modify a Login Method List, click on its corresponding **Edit** button.

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. *xtacacs* - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *local* - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. *none* - Adding this parameter will require no authentication needed to access the Switch.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enable Method Lists Settings

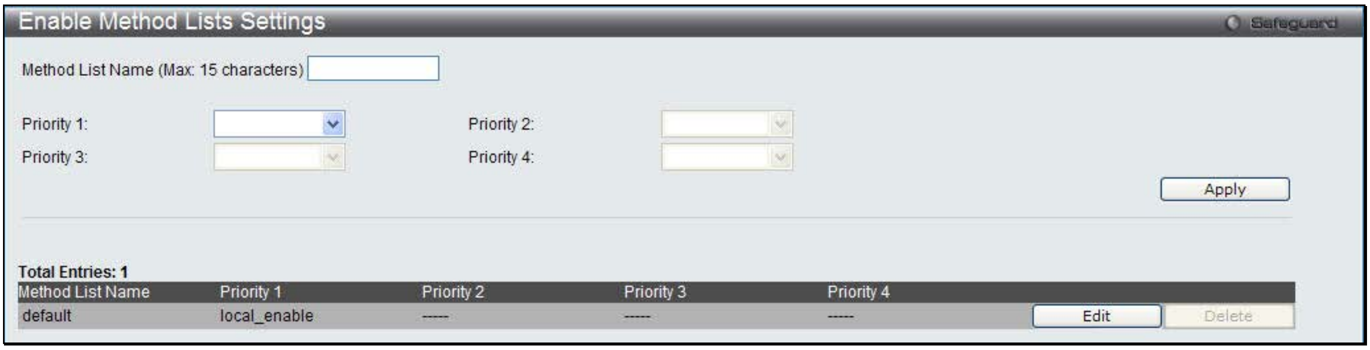
Users can set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.

NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view this window, click **Security > Access Authentication Control > Enable method Lists Settings** as shown below:



Total Entries: 1

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4
default	local_enable	-----	-----	-----

Figure 8-75 Enable method Lists Settings window

To delete an Enable Method List defined by the user, click the **Delete** button corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its corresponding **Edit** button.

The fields that can be configured are described below:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Priority 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication methods to this method list: *local_enable* - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password. *none* - Adding this parameter will require no authentication needed to access the Switch. *radius* - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. *tacacs* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

	xtacacs - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. *tacacs+* - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.

Click the **Apply** button to accept the changes made.

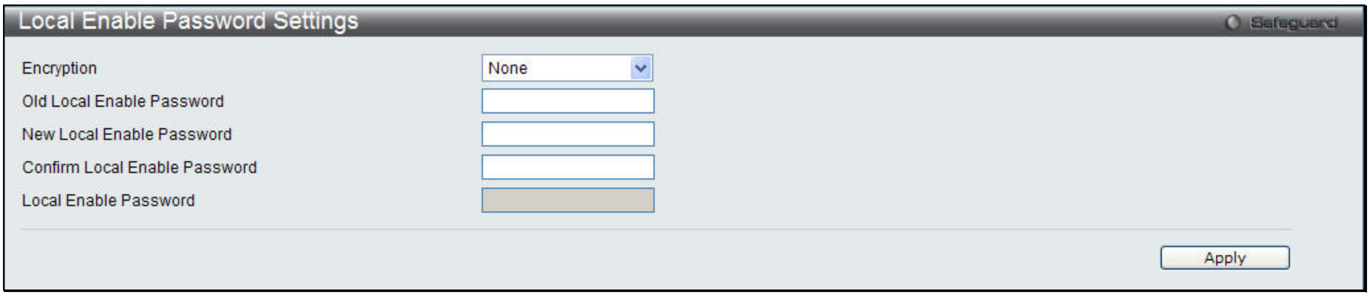
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Local Enable Password Settings

Users can configure the locally enabled password for Enable Admin. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view this window, click **Security > Access Authentication Control > Local Enable Password Settings** as shown below:


Local Enable Password Settings
Safeguard
Old Local Enable Password
New Local Enable Password
Confirm Local Enable Password
Local Enable Password
Apply

Encryption: None

Figure 8-76 Local Enable Password Settings window

The fields that can be configured are described below:

Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click the **Apply** button to accept the changes made.

SSL Settings

Secure Sockets Layer, or SSL, is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

3 **Hash Algorithm:** This part of the cipher suite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

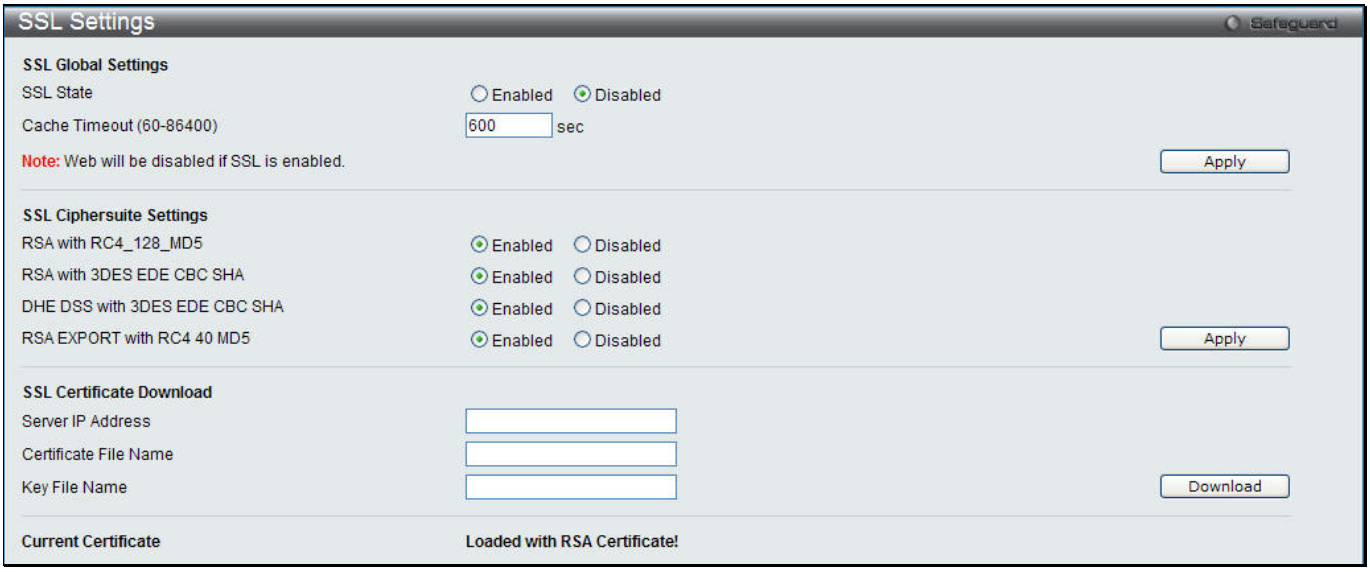
These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

The SSL Settings window located on the next page will allow the user to enable SSL on the Switch and implement any one or combination of listed cipher suites on the Switch. A cipher suite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible cipher suites for the SSL function, which are all enabled by default. To utilize a particular cipher suite, disable the unwanted cipher suites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

To view this window, click **Security > SSL Settings** as shown below:



SSL Settings

SSL Global Settings

SSL State ○ Enabled ● Disabled

Cache Timeout (60-86400) 600 sec

Note: Web will be disabled if SSL is enabled.

SSL Ciphersuite Settings

RSA with RC4_128_MD5 ● Enabled ○ Disabled

RSA with 3DES EDE CBC SHA ● Enabled ○ Disabled

DHE DSS with 3DES EDE CBC SHA ● Enabled ○ Disabled

RSA EXPORT with RC4 40 MD5 ● Enabled ○ Disabled

SSL Certificate Download

Server IP Address

Certificate File Name

Key File Name

Current Certificate Loaded with RSA Certificate!

Figure 8-77 SSL Settings window

To set up the SSL function on the Switch, configure the parameters in the SSL Settings section described.

The fields that can be configured are described below:

Parameter	Description
SSL Status	Use the radio buttons to enable or disable the SSL status on the Switch. The default is Disabled.
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is *600* seconds.

Click the **Apply** button to accept the changes made.

To set up the **SSL cipher suite function** on the Switch, configure the parameters in the SSL Cipher suite Settings section described below:

Parameter	Description
RSA with RC4_128_MD5	This cipher suite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA with 3DES EDE CBC SHA	This cipher suite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
DHS DSS with 3DES EDE CBC SHA	This cipher suite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.
RSA EXPORT with RC4 40 MD5	This cipher suite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the radio buttons to enable or disable this cipher suite. This field is Enabled by default.

Click the **Apply** button to accept the changes made.

To download SSL certificates, configure the parameters in the SSL Certificate Download section described below.

Parameter	Description
Server IP Address	Enter the IPv4 address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Nam	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click the **Download** button to download the SSL certificate based on the information entered.

NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface.

NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SSH

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

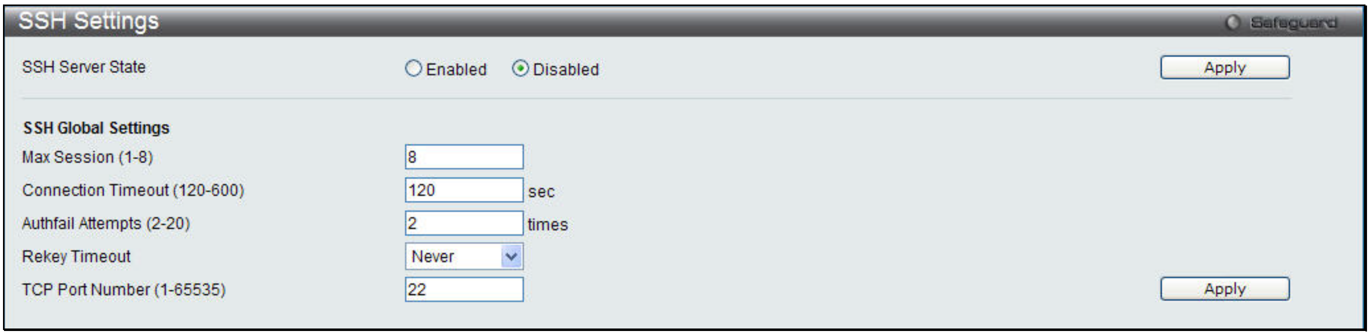
1. Create a user account with admin-level access using the **User Accounts** window. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication Mode** window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password, and Public Key.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the SSH Authentication Method and Algorithm Settings window.
4. Finally, enable SSH on the Switch using the SSH Configuration window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Settings

Users can configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Settings** as shown below:



SSH Server State ○ Enabled ● Disabled

SSH Global Settings

Max Session (1-8): 8

Connection Timeout (120-600): 120 sec

Authfail Attempts (2-20): 2 times

Rekey Timeout: Never

TCP Port Number (1-65535): 22

Figure 8-78 SSH Settings window

The fields that can be configured are described below:

Parameter	Description
SSH Server State	Use the radio buttons to enable or disable SSH on the Switch. The default is Disabled.
Max. Session (1-8)	Enter a value between *1* and *8* to set the number of users that may simultaneously access the Switch. The default setting is *8*.
Connection Timeout (120-600)	Allows the user to set the connection timeout. The user may set a time between *120* and *600* seconds. The default setting is *120* seconds.
Authfail Attempts (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.
Rekey Timeout	This field is used to set the time period that the Switch will change the security shell encryptions by using the drop-down menu. The available options are *Never*, *10 min*,

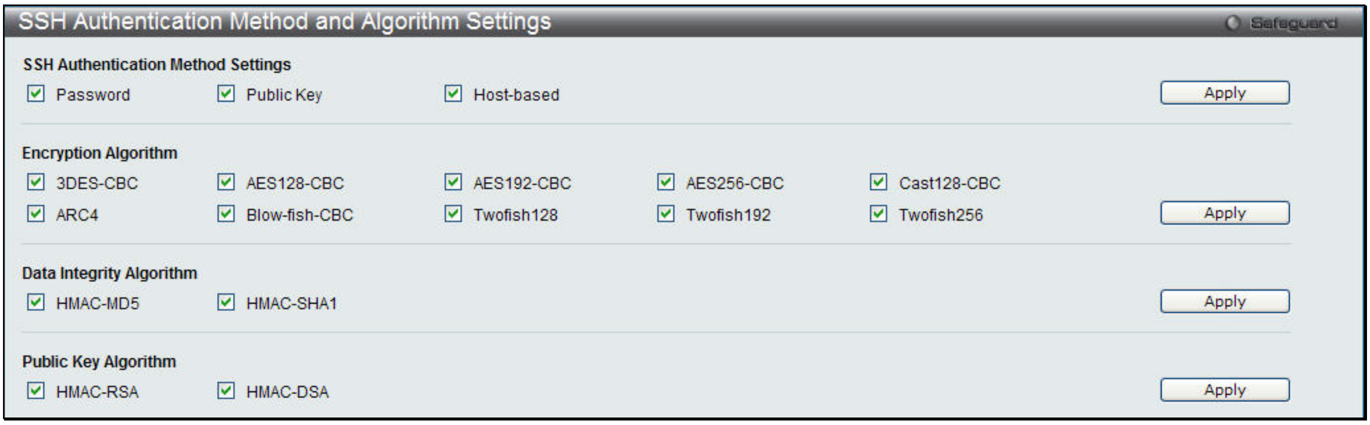
	30 min, and *60 min*. The default setting is *Never*.
TCP Port Number (1-65535)	Here the user can enter the TCP Port Number used for SSH. The default value is *22*.

Click the **Apply** button to accept the changes made for each individual section.

SSH Authentication Method and Algorithm Settings

Users can configure the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by ticking their corresponding check boxes. All algorithms are enabled by default.

To view this window, click **Security > SSH > SSH Authentication method and Algorithm Settings** as shown below:



SSH Authentication Method Settings

☑ Password ☑ Public Key ☑ Host-based

Encryption Algorithm

☑ 3DES-CBC ☑ AES128-CBC ☑ AES192-CBC ☑ AES256-CBC ☑ Cast128-CBC

☑ ARC4 ☑ Blow-fish-CBC ☑ Twofish128 ☑ Twofish192 ☑ Twofish256

Data Integrity Algorithm

☑ HMAC-MD5 ☑ HMAC-SHA1

Public Key Algorithm

☑ HMAC-RSA ☑ HMAC-DSA

Figure 8-79 SSH Authentication Method and Algorithm Settings window

The fields that can be configured for **SSH Authentication Mode** are described below:

Parameter	Description
Password	This may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This parameter is enabled by default.
Public Key	This may be enabled or disabled to choose if the administrator wishes to use a public key configuration set on a SSH server, for authentication. This parameter is enabled by default.
Host-based	This may be enabled or disabled to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This parameter is enabled by default.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Encryption Algorithm** are described below:

Parameter	Description
3DES-CBC	Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.
AES128-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES192-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is enabled.
AES256-CBC	Use the check box to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is enabled.

Cast128-CBC	Use the check box to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is enabled.
ARC4	Use the check box to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is enabled.
Blow-fish CBC	Use the check box to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is enabled.
Twofish128	Use the check box to enable or disable the twofish128 encryption algorithm. The default is enabled.
Twofish192	Use the check box to enable or disable the twofish192 encryption algorithm. The default is enabled.
Twofish256	Use the check box to enable or disable the twofish256 encryption algorithm. The default is enabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Data Integrity Algorithm** are described below:

Parameter	Description
HMAC-MD5	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is enabled.
HMAC-SHA1	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is enabled.

Click the **Apply** button to accept the changes made.

The fields that can be configured for the **Public Key Algorithm** are described below:

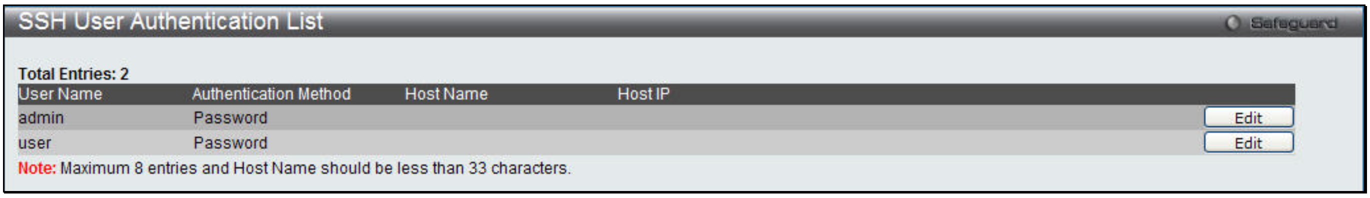
Parameter	Description
HMAC-RSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is enabled.
HMAC-DSA	Use the check box to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is enabled.

Click the **Apply** button to accept the changes made.

SSH User Authentication List

Users can configure parameters for users attempting to access the Switch through SSH. In the window above, the User Account "username" has been previously set using the **User Accounts** window in the **Configuration** folder. A User Account MUST be set in order to set the parameters for the SSH user.

To view this window, click **Security > SSH > SSH User Authentication List** as shown below:



Total Entries: 2

User Name	Authentication Method	Host Name	Host IP
admin	Password		
user	Password		

Note: Maximum 8 entries and Host Name should be less than 33 characters.

Figure 8-80 SSH User Authentication List window

The fields that can be configured or displayed are described below:

Parameter	Description

User Name	A name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Authentication Method	The administrator may choose one of the following to set the authorization for users attempting to access the Switch. *Host Based* – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. *Password* – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation. *Public Key* – This parameter should be chosen if the administrator wishes to use the public key on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the **Host Based** choice in the **Authentication Mode** field.

Click the **Edit** button to re-configure the specific entry.

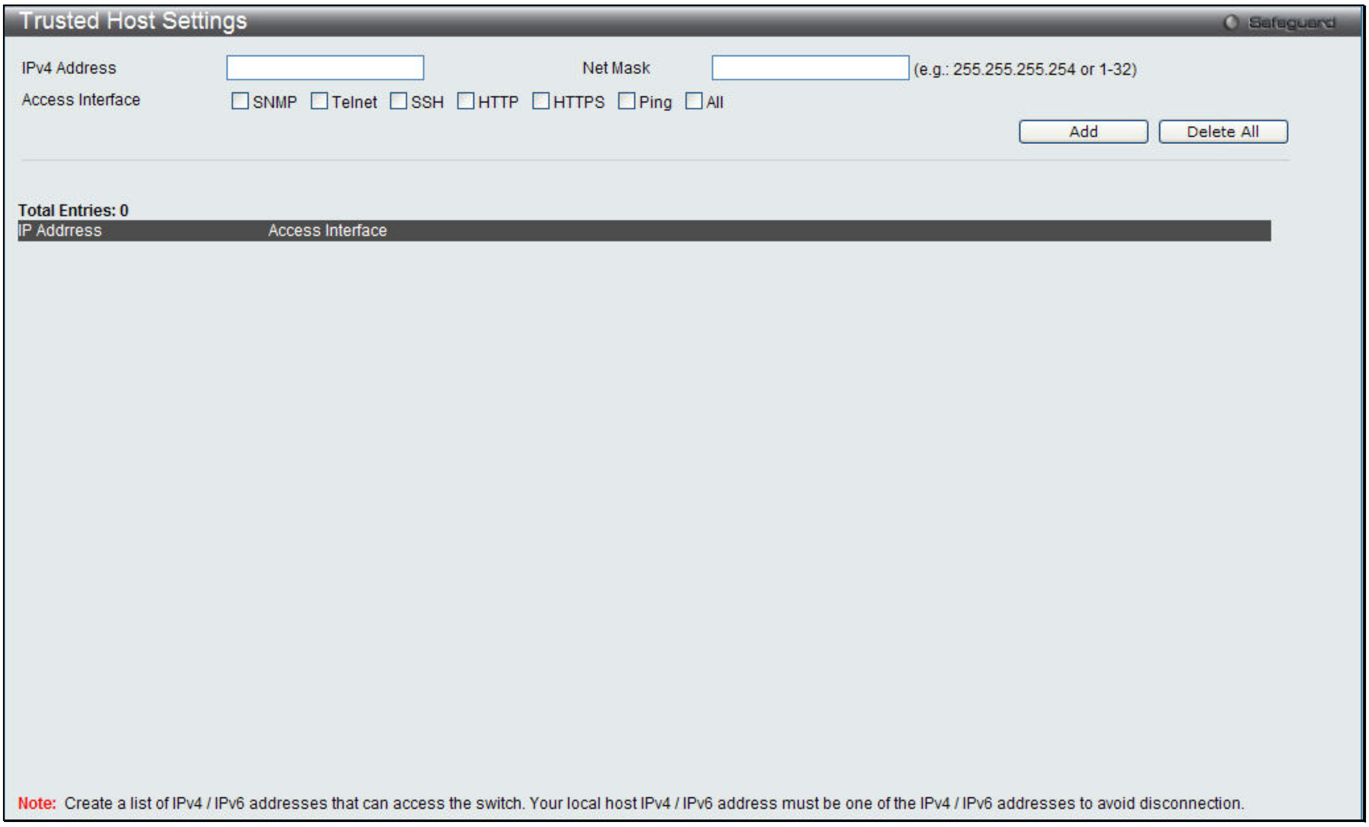
Click the **Apply** button to accept the changes made.

NOTE: To set the SSH User Authentication Mode parameters on the Switch, a User Account must be previously configured.

Trusted Host Settings

Up to thirty trusted host secure IP addresses or ranges may be configured and used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

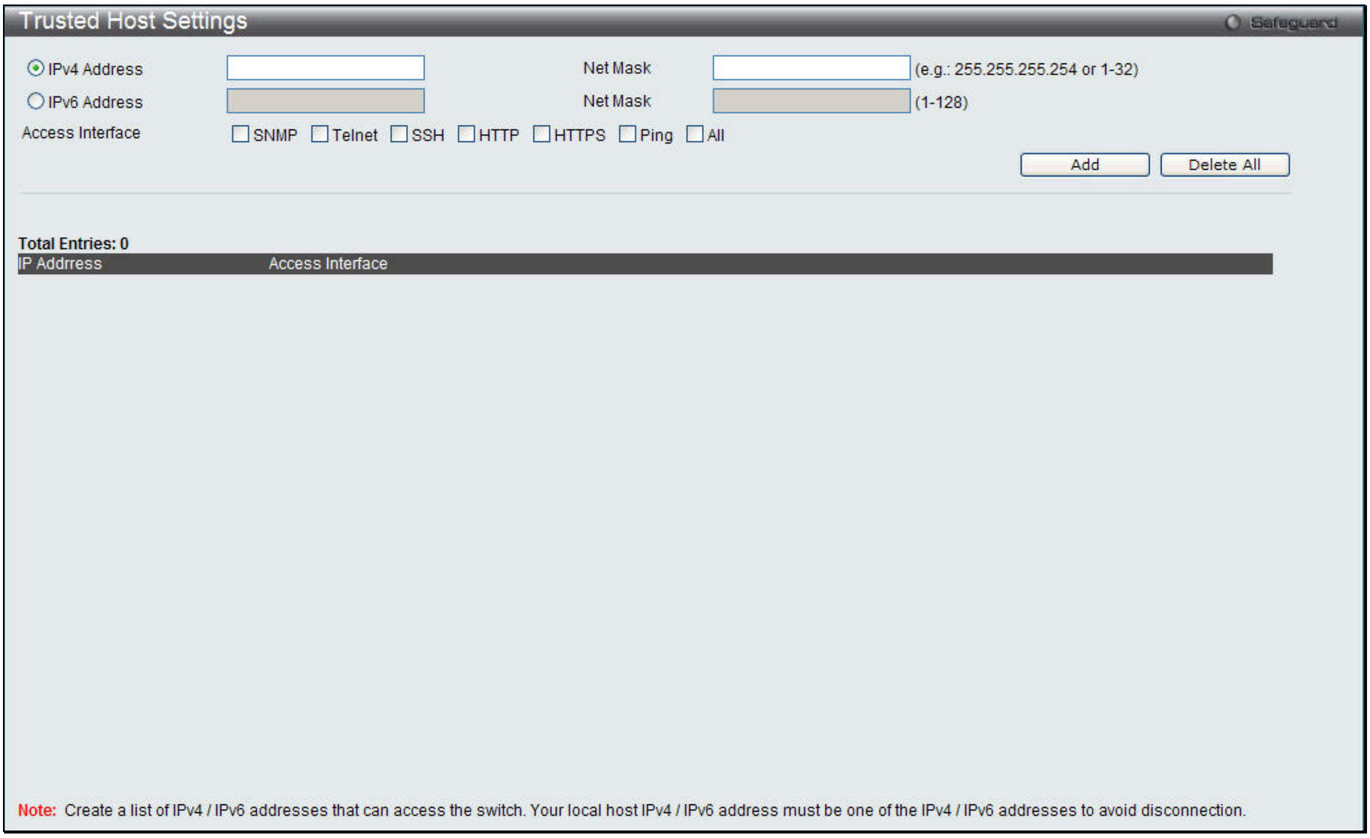
To view this window, click **Security > Trusted Host Settings** as shown below:


Trusted Host Settings
Safeguard
IPv4 Address
Net Mask
(e.g.: 255.255.255.254 or 1-32)
Access Interface
☐ SNMP ☐ Telnet ☐ SSH ☐ HTTP ☐ HTTPS ☐ Ping ☐ All
Add
Delete All
IP Address
Access Interface

Total Entries: 0

Note: Create a list of IPv4 / IPv6 addresses that can access the switch. Your local host IPv4 / IPv6 address must be one of the IPv4 / IPv6 addresses to avoid disconnection.

Figure 8-81 Trusted Host window (SI Mode Only)


Trusted Host Settings
Safeguard
● IPv4 Address
Net Mask
(e.g.: 255.255.255.254 or 1-32)
○ IPv6 Address
Net Mask
(1-128)
Access Interface
☐ SNMP ☐ Telnet ☐ SSH ☐ HTTP ☐ HTTPS ☐ Ping ☐ All
Add
Delete All
IP Address
Access Interface

Total Entries: 0

Note: Create a list of IPv4 / IPv6 addresses that can access the switch. Your local host IPv4 / IPv6 address must be one of the IPv4 / IPv6 addresses to avoid disconnection.

Figure 8-82 Trusted Host window (EI Mode Only)

When the user clicks the **Edit** button, one will be able to edit the service allowed to the selected host.

The fields that can be configured are described below:

Parameter	Description

IPv4 Address	Enter an IPv4 address to add to the trusted host list.
IPv6 Address (EI Mode Only)	Enter an IPv6 address to add to the trusted host list.
Net Mask	Enter a Net Mask address to add to the trusted host list.
Access Interface	Tick the check boxes to select services that will be allowed to the trusted host.

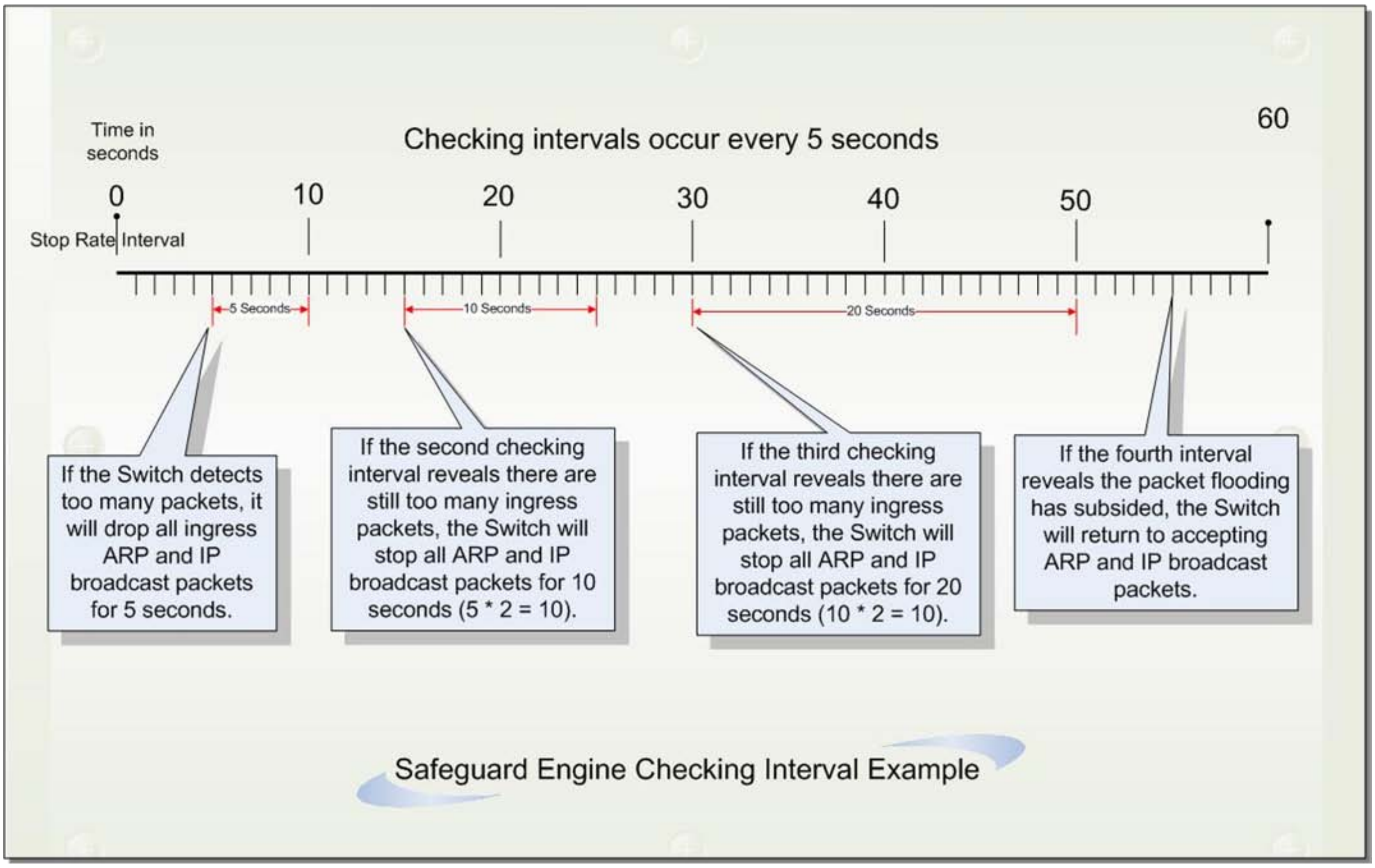
Click the **Add** button to add a new entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

Safeguard Engine Settings

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. The Safeguard Engine has two operating modes that can be configured by the user, *Strict* and *Fuzzy*. In *Strict* mode, when the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter the Exhausted mode. When in this mode, the Switch will drop all ARP and IP broadcast packets and packets from un-trusted IP addresses for a calculated time interval. Every five seconds, the Safeguard Engine will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will initially stop all ingress ARP and IP broadcast packets and packets from un-trusted IP addresses for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will stop accepting all ARP and IP broadcast packets and packets from un-trusted IP addresses for double the time of the previous stop period. This doubling of time for stopping these packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds. For a better understanding, please examine the following example of the Safeguard Engine.



If the Switch detects too many packets, it will drop all ingress ARP and IP broadcast packets for 5 seconds.

If the second checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 10 seconds (5 * 2 = 10).

If the third checking interval reveals there are still too many ingress packets, the Switch will stop all ARP and IP broadcast packets for 20 seconds (10 * 2 = 10).

If the fourth interval reveals the packet flooding has subsided, the Switch will return to accepting ARP and IP broadcast packets.

Safeguard Engine Checking Interval Example

Figure 8-83 Mapping QoS on the Switch

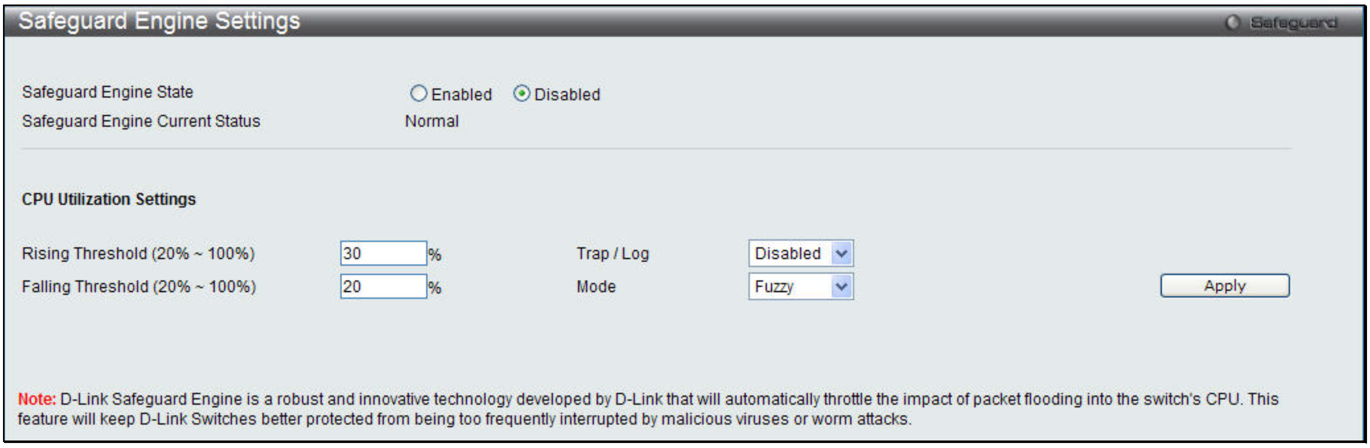
For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will discard ingress ARP and IP broadcast packets and packets from the illegal IP addresses. In the example above, the Switch doubled the time for dropping ARP and IP broadcast packets when consecutive flooding issues were detected at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for dropping ARP and IP broadcast packets will return to 5 seconds and the process will resume.

In *Fuzzy* mode, once the Safeguard Engine has entered the Exhausted mode, the Safeguard Engine will decrease the packet flow by half. After returning to Normal mode, the packet flow will be increased by 25%. The switch will then return to its interval checking and dynamically adjust the packet flow to avoid overload of the Switch.

NOTICE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Users can enable the Safeguard Engine or configure advanced Safeguard Engine settings for the Switch.

To view this window, click **Security > Safeguard Engine Settings** as shown below:



Safeguard Engine Settings

Safeguard Engine State ○ Enabled ● Disabled

Safeguard Engine Current Status Normal

CPU Utilization Settings

Rising Threshold (20% ~ 100%) 30 %

Falling Threshold (20% ~ 100%) 20 %

Trap / Log Disabled

Mode Fuzzy

Note: D-Link Safeguard Engine is a robust and innovative technology developed by D-Link that will automatically throttle the impact of packet flooding into the switch's CPU. This feature will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

Figure 8-84 Safeguard Engine Settings window

The fields that can be configured are described below:

Parameter	Description
Safeguard Engine State	Use the radio button to globally enable or disable Safeguard Engine settings for the Switch.
Rising Threshold (20% - 100%)	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.
Falling Threshold (20% - 100%)	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.
Trap / Log	Use the drop-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: *Fuzzy* – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. *Strict* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided. The default setting is *Fuzzy* mode.

Click the **Apply** button to accept the changes made.

Chapter 9 Network Application

DHCP
PPPoE Circuit ID Insertion Settings (EI Mode Only)
SMTP Settings
SNTP
Flash File System Settings

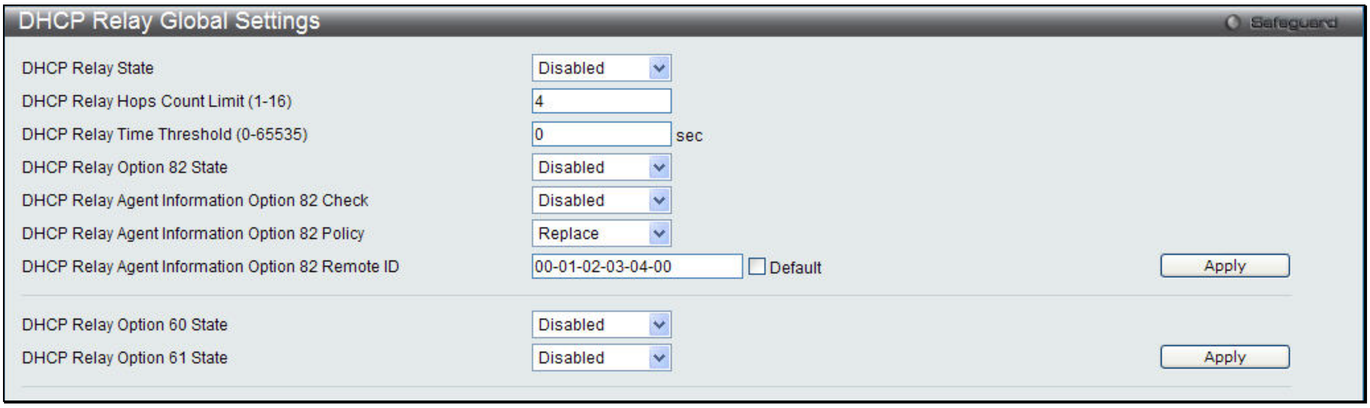
DHCP

DHCP Relay

DHCP Relay Global Settings

This window is used to enable and configure DHCP Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between *1* and *16* hops, with a default value of *4*. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds' field of the packet is less than the relay time threshold, the packet will be dropped. The range is between *0* and *65,535* seconds, with a default value of *0* seconds.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Global Settings** as shown below:



DHCP Relay State	Disabled
DHCP Relay Hops Count Limit (1-16)	4
DHCP Relay Time Threshold (0-65535)	0 sec
DHCP Relay Option 82 State	Disabled
DHCP Relay Agent Information Option 82 Check	Disabled
DHCP Relay Agent Information Option 82 Policy	Replace
DHCP Relay Agent Information Option 82 Remote ID	00-01-02-03-04-00 ☐ Default
DHCP Relay Option 60 State	Disabled
DHCP Relay Option 61 State	Disabled

Figure 9-1 DHCP Relay Global Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Relay State	Use the drop-down menu to enable or disable the DHCP Relay service on the Switch. The default is *Disabled.*
DHCP Relay Hops Count Limit (1-16)	Enter an entry between *1* and *16* to define the maximum number of router hops DHCP messages can be forwarded. The default hop count is *4*.
DHCP Relay Time Threshold (0-65535)	Enter an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP packet. If a value of *0* is entered, the Switch will not process the value in the seconds' field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.
DHCP Relay Option 82 State	Use the drop-down menu to enable or disable the DHCP Relay Agent Information Option 82 on the Switch. The default is *Disabled.* *Enabled* –When this field is toggled to *Enabled*, the relay agent will insert and

	remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *Disabled*- When the field is toggled to *Disabled*, the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	Use the drop-down menu to enable or disable the Switches ability to check the validity of the packet's option 82 field. *Enabled* – When the field is toggled to *Enabled*, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *Disabled* – When the field is toggled to *Disabled*, the relay agent will not check the validity of the packet's option 82 field.
DHCP Relay Agent Information Option 82 Policy	Use the drop-down menu to set the Switches policy for handling packets when the DHCP Relay Agent Information Option 82 Check is set to *Disabled*. The default is *Replace.* *Replace* – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *Drop* – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *Keep* – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	Enter the DHCP Relay Agent Information Option 82 Remote ID.
DHCP Relay Option 60 State	Use the drop-down menu to enable or disable the use of the DHCP Relay Option 60 State feature. If the packet does not have option 60 enabled, then the relay servers cannot be determined based on the option 60. In this case the relay servers will be determined based on either option 61 or per IPIF configured servers. If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined by either option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers. *enable* – Select this option to enable the DHCP Relay Option 60 state, in order to relay DHCP packets. *disable* - Select this option to disable the DHCP Relay Option 60 state.
DHCP Relay Option 61 State	Use the drop-down menu to enable or disable the use of the DHCP Relay Option 61 State feature. When option 61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers. *enable* – Select this option to enable the DHCP Relay Option 61 state, in order to relay DHCP packets. *disable* - Select this option to disable the DHCP Relay Option 61 state.

Click the **Apply** button to accept the changes made for each individual section.

NOTE: If the Switch receives a packet that contains the option 82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option 82 field. In this situation, disable the information check feature so that the Switch does not remove the option 82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option 82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Relay Agent Information Option 82

The **DHCP Relay Option 82** command configures the DHCP relay agent information option 82 setting of the Switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:

NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

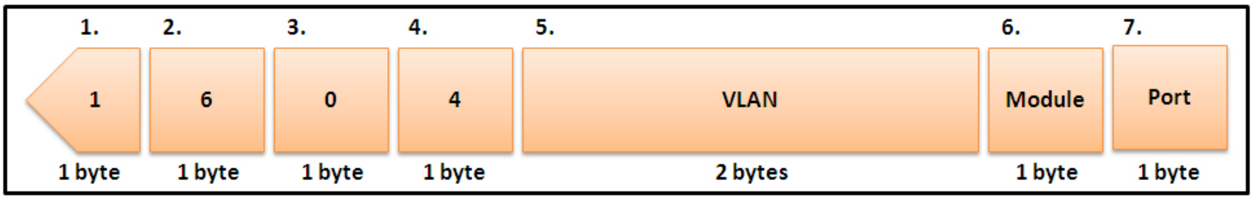


Figure 9-2 Circuit ID Sub-option Format

1 Sub-option type
2 Length
3 Circuit ID type
4 Length
5 VLAN: The incoming VLAN ID of DHCP client packet.
6 Module: For a standalone switch, the Module is always 0; for a stackable switch, the Module is the Unit ID.
7 Port: The incoming port number of the DHCP client packet, the port number starts from 1.

Remote ID sub-option format:

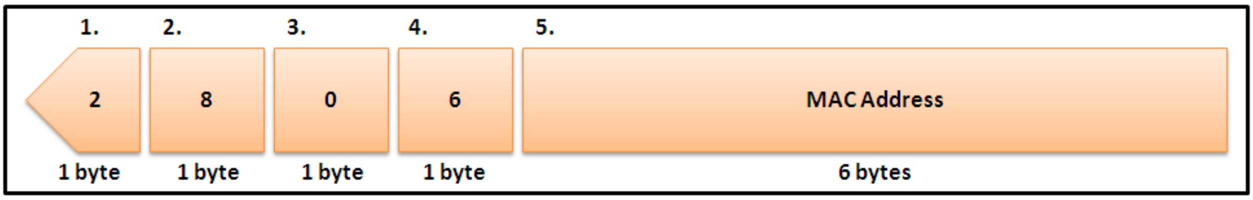


Figure 9-3 Remote ID Sub-option Format

1 Sub-option type
2 Length
3 Remote ID type
4 Length
5 MAC address: The Switch’s system MAC address.

DHCP Relay Interface Settings

This window is used to set up a server, by IP address, for relaying DHCP information to the Switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP server using this window. Properly configured settings will be displayed in the DHCP Relay Interface Table at the bottom of the window, once the user clicks the **Apply** button. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking the corresponding **Delete** button.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Interface Settings** as shown below:

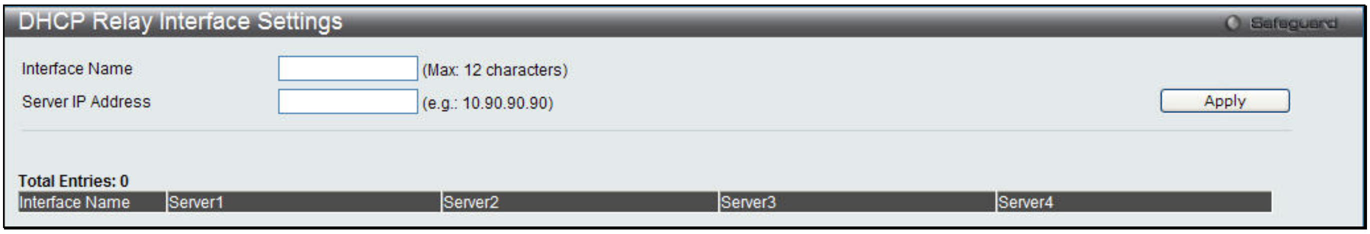

DHCP Relay Interface Settings
Safeguard
Interface Name
(Max: 12 characters)
Server IP Address
(e.g.: 10.90.90.90)
Apply
Total Entries: 0
Interface Name
Server1
Server2
Server3
Server4

Figure 9-4 DHCP Relay Interface Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	The IP interface on the Switch that will be connected directly to the Server.
Server IP Address	Enter the IP address of the DHCP server. Up to four server IPs can be configured per IP Interface.

Click the **Apply** button to accept the changes made.

DHCP Relay VLAN Settings

This window is used to configure an IP address as a destination to forward (relay) DHCP/BOOTP packets. If there is an IP interface in the VLAN and it has configured a DHCP server at the interface level, then the configuration at the interface level has higher priority. In this case, the DHCP server configured on the VLAN will not be used to forward the DHCP packets.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay VLAN Settings** as shown below:

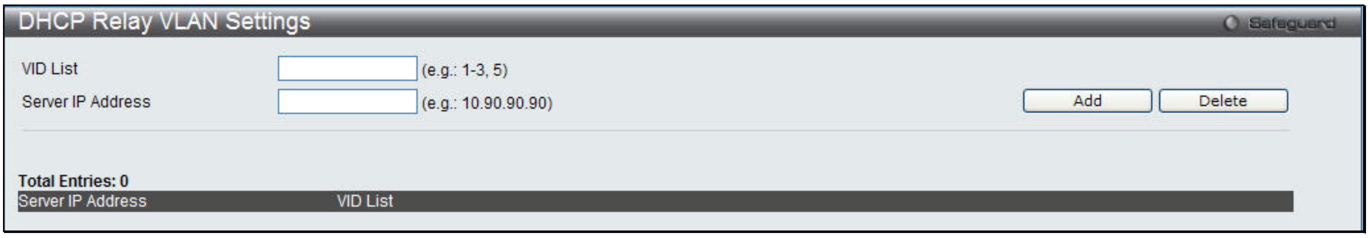

DHCP Relay VLAN Settings
Safeguard
VID List
(e.g.: 1-3, 5)
Server IP Address
(e.g.: 10.90.90.90)
Add
Delete
Total Entries: 0
Server IP Address
VID List

Figure 9-5 DHCP Relay VLAN Settings window

The fields that can be configured are described below:

Parameter	Description
VID List	Enter the VLAN ID list used for this configuration here.
Server IP Address	Enter the DHCP/BOOTP server IP address used here.

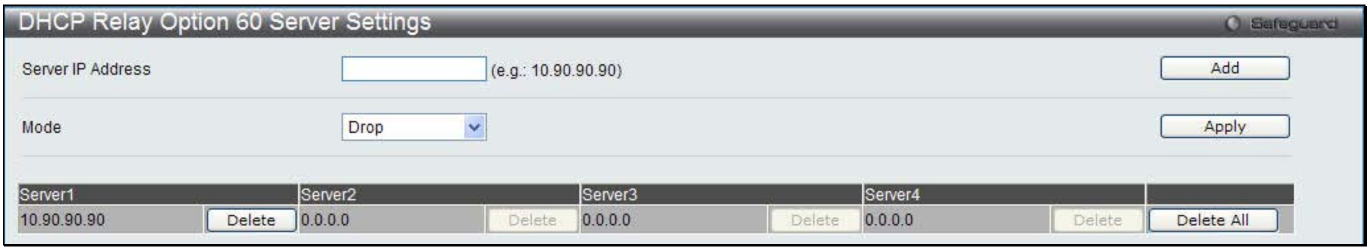
Click the **Add** button to add an entry.

Click the **Delete** button to remove an entry.

DHCP Relay Option 60 Server Settings

This window is used to configure the DHCP relay option 60 server parameters.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Server Settings** as shown below:


DHCP Relay Option 60 Server Settings
Safeguard
Server IP Address
(e.g.: 10.90.90.90)
Add
Mode
Apply
Delete
Delete All

Mode: Drop

Server1		Server2		Server3		Server4		
10.90.90.90	Delete	0.0.0.0	Delete	0.0.0.0	Delete	0.0.0.0	Delete	Delete All

Figure 9-6 DHCP Relay Option 60 Server Settings window

The fields that can be configured are described below:

Parameter	Description
Server IP Address	Enter the DHCP Relay Option 60 Server Relay IP Address.
Mode	Use the drop-down menu to select the DHCP Relay Option 60 Server mode.

Click the **Add** button to add a new entry based on the information entered.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specific entry.

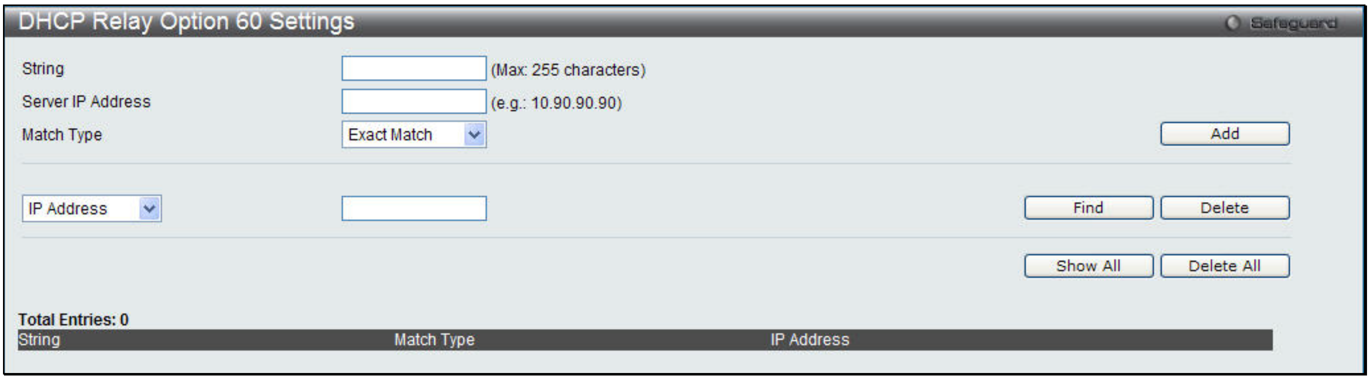
Click the **Delete All** button to remove all the entries listed.

NOTE: When there is no matching server found for the packet based on option 60, the relay servers will be determined by the default relay server setting.

DHCP Relay Option 60 Settings

This option decides whether the DHCP Relay will process the DHCP option 60 or not

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings** as shown below:


DHCP Relay Option 60 Settings
Safeguard
String
(Max: 255 characters)
Server IP Address
(e.g.: 10.90.90.90)
Match Type
Add
Find
Delete
Show All
Delete All
String
Match Type
IP Address

Match Type: Exact Match

IP Address

Total Entries: 0

Figure 9-7 DHCP Relay Option 60 Settings window

The fields that can be configured are described below:

Parameter	Description
String	Enter the DHCP Relay Option 60 String value. Different strings can be specified for the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.

Server IP Address	Here the user can enter the DHCP Relay Option 60 Server IP address.
Match Type	Here the user can enter the DHCP Relay Option 60 Match Type value. *Exact Match* – The option 60 string in the packet must full match with the specified string. *Partial Match* – The option 60 string in the packet only need partial match with the specified string.
IP Address	Enter the DHCP Relay Option 60 IP address.
String	Enter the DHCP Relay Option 60 String value.

Click the **Add** button to add a new entry based on the information entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

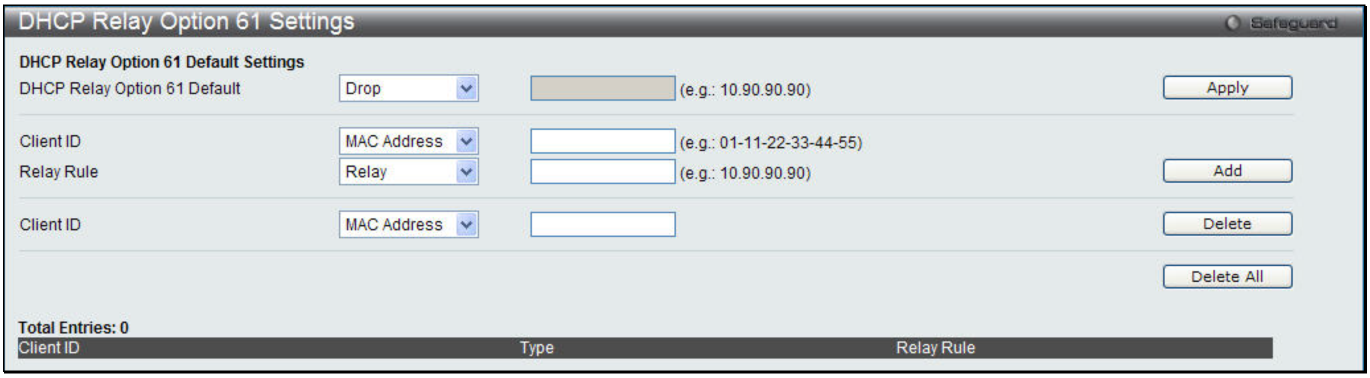
Click the **Show All** button to display all the existing entries.

Click the **Delete All** button to remove all the entries listed.

DHCP Relay Option 61 Settings

This window is used to configure, add and delete DHCP relay option 61 parameters.

To view this window, click **Network Application > DHCP > DHCP Relay > DHCP Relay Option 61 Settings** as shown below:



DHCP Relay Option 61 Settings

DHCP Relay Option 61 Default Settings

DHCP Relay Option 61 Default: Drop (e.g.: 10.90.90.90)

Client ID: MAC Address (e.g.: 01-11-22-33-44-55)

Relay Rule: Relay (e.g.: 10.90.90.90)

Client ID: MAC Address

Total Entries: 0

Client ID	Type	Relay Rule

Figure 9-8 DHCP Relay Option 61 Settings window

The fields that can be configured are described below:

Parameter	Description
DHCP Relay Option 61 Default	Here the user can select the DHCP Relay Option 61 default action. *Drop* – Specify to drop the packet. *Relay* – Specify to relay the packet to an IP address. Enter the IP Address of the default relay server. When there is no matching server found for the packet based on option 61, the relay servers will be determined by this default relay server setting.
Client ID	*MAC Address* – The client’s client-ID which is the hardware address of client. *String* – The client’s client-ID, which is specified by administrator.
Relay Rule	*Drop* – Specify to drop the packet. *Relay* – Specify to relay the packet to an IP address.
Client ID	*MAC Address* – The client’s client-ID which is the hardware address of client. *String* – The client’s client-ID, which is specified by administrator.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specific entry based on the information entered.

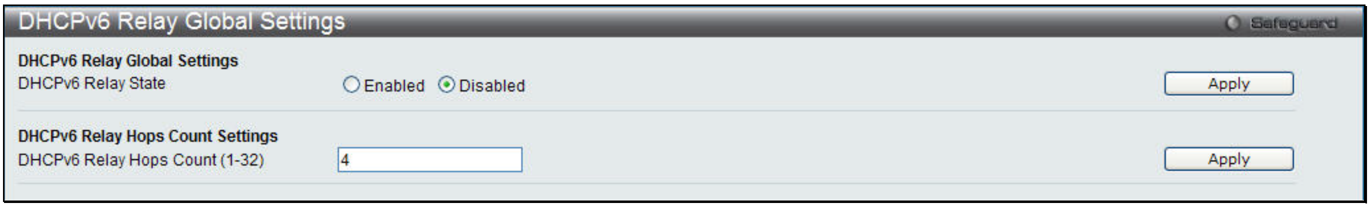
Click the **Delete All** button to remove all the entries listed.

DHCPv6 Relay (EI Mode Only)

DHCPv6 Relay Global Settings

This window is used to configure the DHCPv6 relay function.

To view this window, click **Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings** as shown below:



DHCPv6 Relay Global Settings

DHCPv6 Relay State ○ Enabled ● Disabled

DHCPv6 Relay Hops Count Settings

DHCPv6 Relay Hops Count (1-32) 4

Figure 9-9 DHCPv6 Relay Global Settings window

The fields that can be configured are described below:

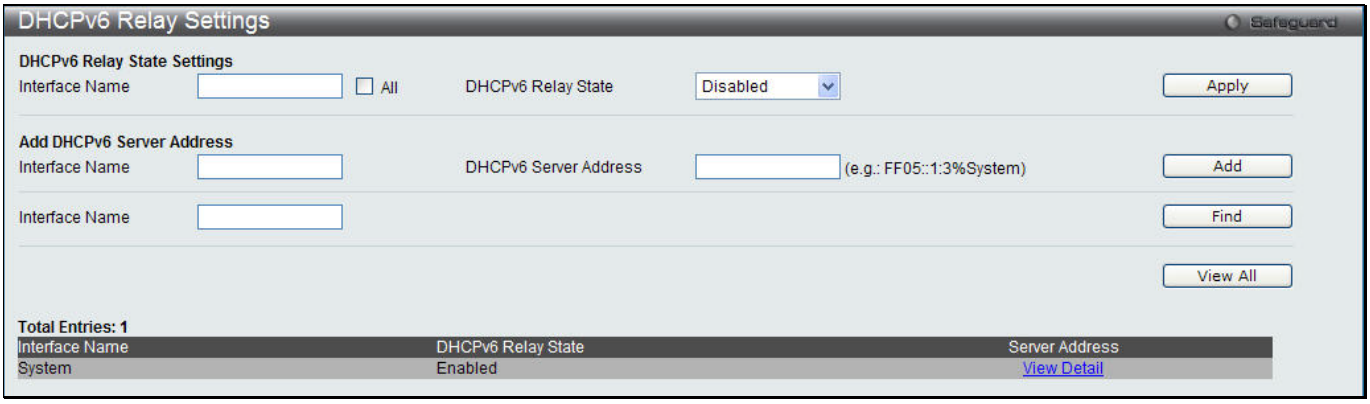
Parameter	Description
DHCPv6 Relay State	Click the radio buttons to enable or disable the DHCPv6 relay function.
DHCPv6 Relay Hops Count (1-32)	Enter the number of relay agents that have to be relayed in this message. The default value is *4*.

Click the **Apply** button to accept the changes made for each individual section.

DHCPv6 Relay Settings

This window is used to configure the DHCPv6 relay state of one or all of the specified interfaces, and add or display a destination IPv6 address to or from the switch's DHCPv6 relay table.

To view this window, click **Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Settings** as shown below:



DHCPv6 Relay State Settings

Interface Name ☐ All DHCPv6 Relay State Disabled

Add DHCPv6 Server Address

Interface Name DHCPv6 Server Address (e.g.: FF05::1:3%System)

Interface Name

Total Entries: 1

Interface Name	DHCPv6 Relay State	Server Address
System	Enabled	View Detail

Figure 9-10 DHCPv6 Relay Settings window

The fields that can be configured are described below:

Parameter	Description
Interface Name	Enter the name of the IPv6 interface. Tick the **All** check box to select all IPv6 interfaces.
DHCPv6 Relay State	Use the drop-down menu to enable or disable the DHCPv6 relay state of the interface.
DHCPv6 Server	Enter the DHCPv6 server IPv6 address.

Address	

Click the **Apply** button to accept the changes made.

Click the **Add** button to add an entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **View All** button to display all the existing entries.

Click the View Detail link to view more information regarding the specific entry.

After clicking the View Detail link, the following page will appear:

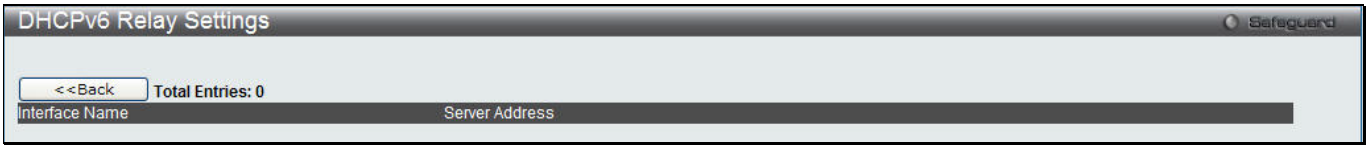

DHCPv6 Relay Settings
Safeguard
<<Back
Total Entries: 0
Interface Name
Server Address

Figure 9-11 DHCPv6 Relay Settings - View Detail window

Click the **<<Back** button to discard the changes made and return to the previous page.

DHCP Local Relay Settings

The DHCP local relay settings allows the user to add option 82 into DHCP request packets when the DHCP client gets an IP address from the same VLAN. If the DHCP local relay settings are not configured, the Switch will flood the packets to the VLAN. In order to add option 82 into the DHCP request packets, the DHCP local relay settings and the state of the Global VLAN need to be enabled.

To view this window, click **Network Application > DHCP > DHCP Local Relay Settings** as shown below:

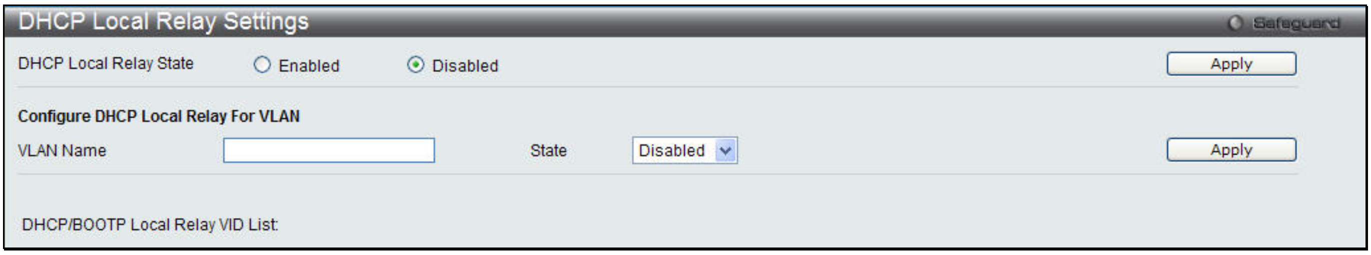

DHCP Local Relay Settings
Safeguard
DHCP Local Relay State
○ Enabled
● Disabled
Apply
Configure DHCP Local Relay For VLAN
VLAN Name
State
Disabled
Apply
DHCP/BOOTP Local Relay VID List

Figure 9-12 DHCP Local Relay Settings window

The fields that can be configured are described below:

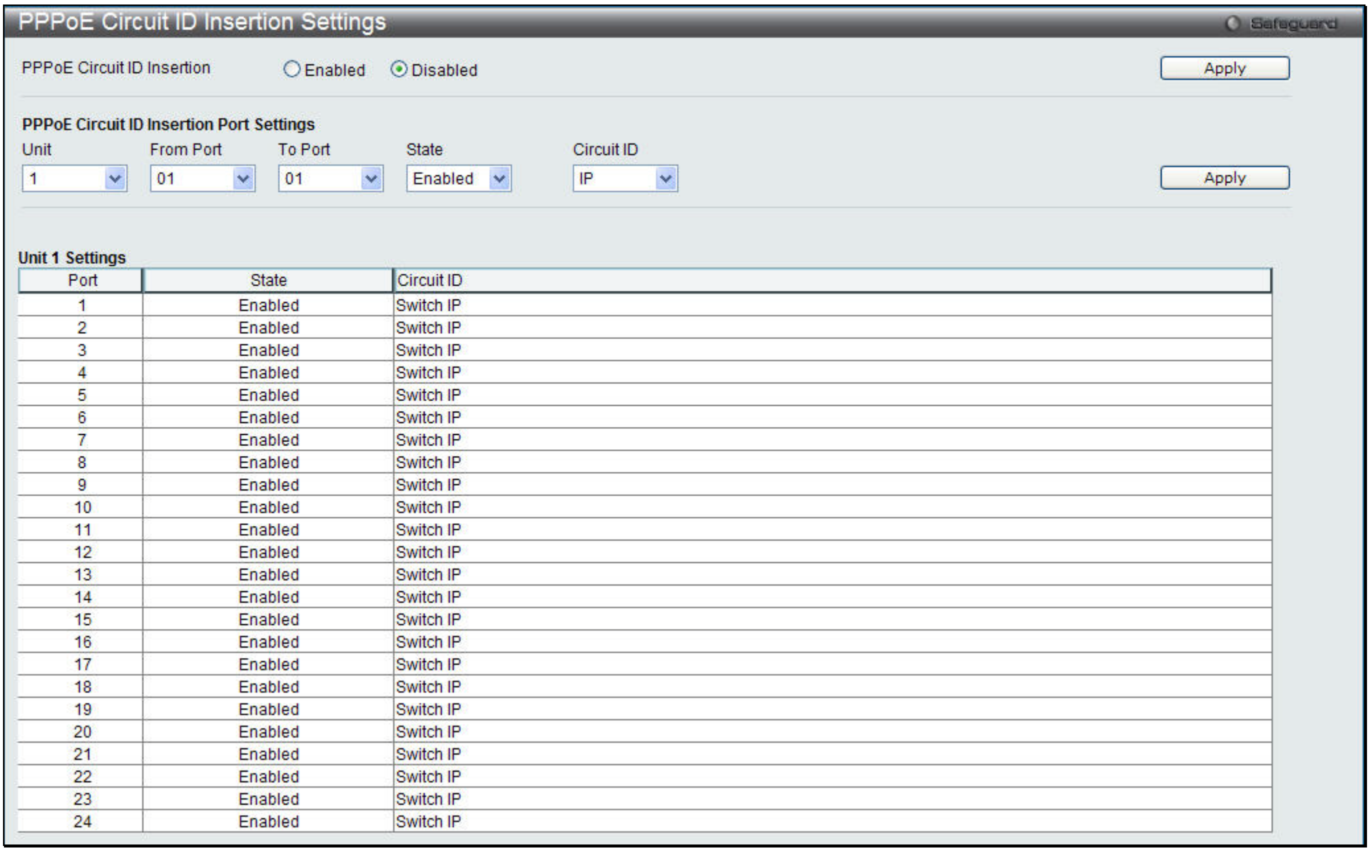
Parameter	Description
DHCP Local Relay State	Enable or disable the DHCP Local Relay Global State. The default is Disabled.
VLAN Name	This is the VLAN Name that identifies the VLAN the user wishes to apply the DHCP Local Relay operation.
State	Enable or disable the configure DHCP Local Relay for VLAN state.

Click the **Apply** button to accept the changes made for each individual section.

PPPoE Circuit ID Insertion Settings (EI Mode Only)

This window is used to configure the PPPoE circuit ID insertion function.

To view this window, click **Network Application > PPPoE Circuit ID Insertion Settings** as shown below:



PPPoE Circuit ID Insertion Settings

PPPoE Circuit ID Insertion ○ Enabled ● Disabled

PPPoE Circuit ID Insertion Port Settings

Unit	From Port	To Port	State	Circuit ID
1	01	01	Enabled	IP

Unit 1 Settings

Port	State	Circuit ID
1	Enabled	Switch IP
2	Enabled	Switch IP
3	Enabled	Switch IP
4	Enabled	Switch IP
5	Enabled	Switch IP
6	Enabled	Switch IP
7	Enabled	Switch IP
8	Enabled	Switch IP
9	Enabled	Switch IP
10	Enabled	Switch IP
11	Enabled	Switch IP
12	Enabled	Switch IP
13	Enabled	Switch IP
14	Enabled	Switch IP
15	Enabled	Switch IP
16	Enabled	Switch IP
17	Enabled	Switch IP
18	Enabled	Switch IP
19	Enabled	Switch IP
20	Enabled	Switch IP
21	Enabled	Switch IP
22	Enabled	Switch IP
23	Enabled	Switch IP
24	Enabled	Switch IP

Figure 9-13 PPPoE Circuit ID Insertion Settings window

The fields that can be configured are described below:

Parameter	Description
PPPoE Circuit ID Insertion	Click the radio buttons to enable or disable the PPPoE circuit ID insertion on the Switch.
Unit	Use the drop-down menus to select a unit to be configured.
From Port / To Port	Use the drop-down menus to select a range of ports to be configured.
State	Use the drop-down menu to enable or disable port's PPPoE circuit ID insertion function.
Circuit ID	Use the drop-down menu to select the device ID part for encoding of the circuit ID option.

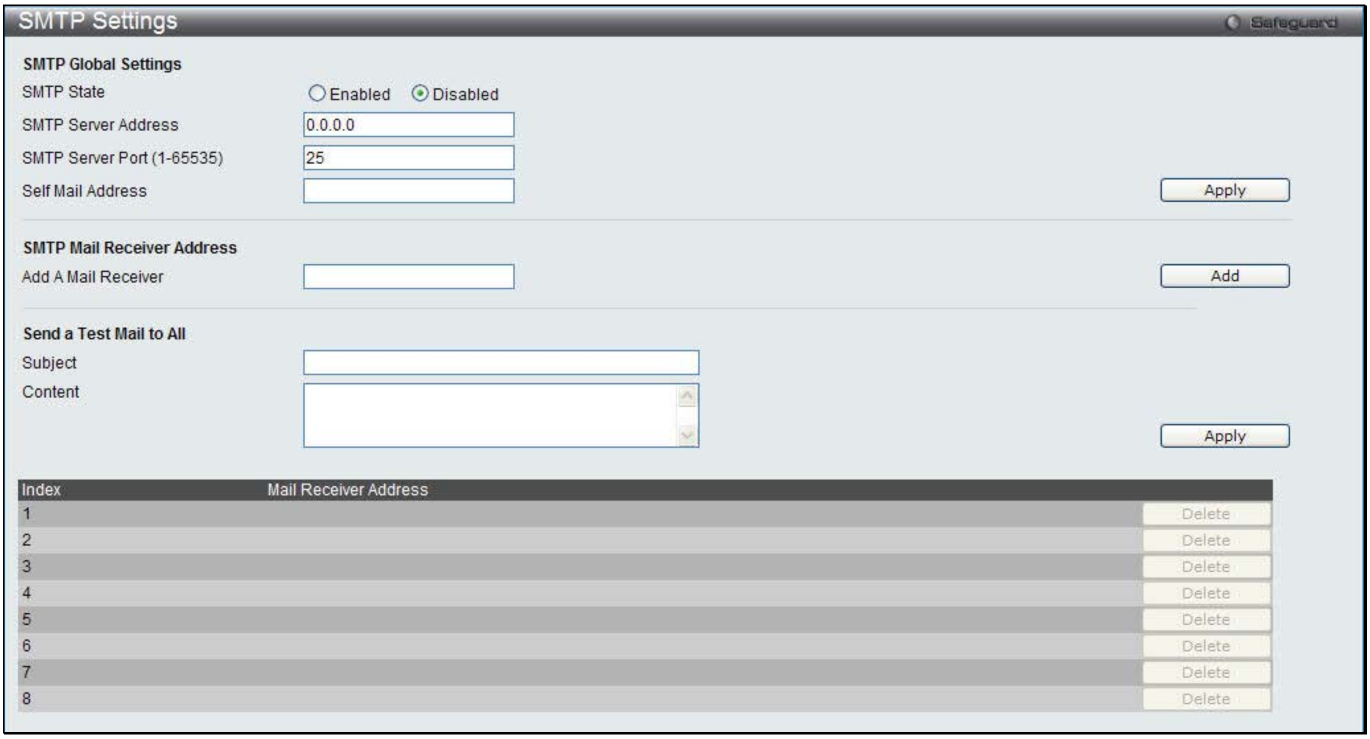
Click the **Apply** button to accept the changes made for each individual section.

SMTP Settings

SMTP or Simple Mail Transfer Protocol is a function of the Switch that will send switch events to mail recipients based on e-mail addresses entered in the window below. The Switch is to be configured as a client of SMTP while the server is a remote device that will receive messages from the Switch, place the appropriate information into an e-mail and deliver it to recipients configured on the Switch. This can benefit the Switch administrator by simplifying the management of small workgroups or wiring closets, increasing the speed of handling emergency Switch events, and enhancing security by recording questionable events occurring on the Switch.

Users can set up the SMTP server for the Switch, along with setting e-mail addresses to which switch log files can be sent when a problem arises on the Switch.

To view this window, click **Network Application > SMTP Settings** as shown below:



SMTP Global Settings

SMTP State ○ Enabled ● Disabled

SMTP Server Address 0.0.0.0

SMTP Server Port (1-65535) 25

Self Mail Address

SMTP Mail Receiver Address

Add A Mail Receiver

Send a Test Mail to All

Subject

Content

Index	Mail Receiver Address	
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete
6		Delete
7		Delete
8		Delete

Figure 9-14 SMTP Settings window

The fields that can be configured are described below:

Parameter	Description
SMTP State	Use the radio button to enable or disable the SMTP service on this device.
SMTP Server Address	Enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for you.
SMTP Server Port (1-65535)	Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is 25, yet a value between 1 and 65535 can be chosen.
Self Mail Address	Enter the e-mail address from which mail messages will be sent. This address will be the “from” address on the e-mail message sent to a recipient. Only one self-mail address can be configured for this Switch. This string can be no more that 64 alphanumeric characters.
Add A Mail Receiver	Enter an e-mail address and click the **Add** button. Up to eight e-mail addresses can be added per Switch. To delete these addresses from the Switch, click the corresponding Delete button in the SMTP Mail Receiver Address table at the bottom of the window.
Subject	Enter the title of the testing mail.
Content	Enter the content of the testing mail.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Add** button to add an entry.

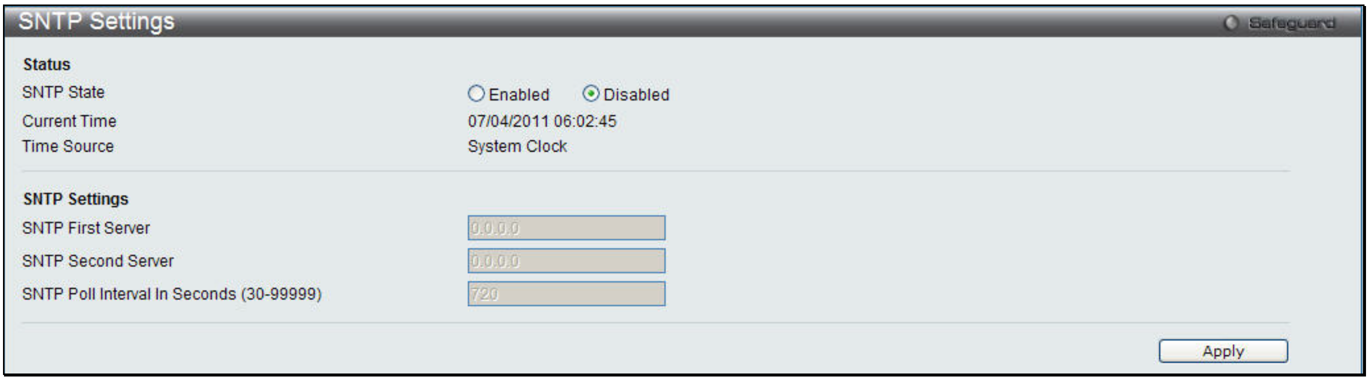
SNTP

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the SNTP subnet of servers and clients, and adjust the system clock in each participant.

SNTP Settings

Users can configure the time settings for the Switch.

To view this window, click **Network Application > SNTP > SNTP Settings** as shown below:



Status

SNTP State: ○ Enabled ● Disabled
Current Time: 07/04/2011 06:02:45
Time Source: System Clock

SNTP Settings

SNTP First Server: 0.0.0.0
SNTP Second Server: 0.0.0.0
SNTP Poll Interval In Seconds (30-99999): 720

Figure 9-15 SNTP Settings window

The fields that can be configured are described below:

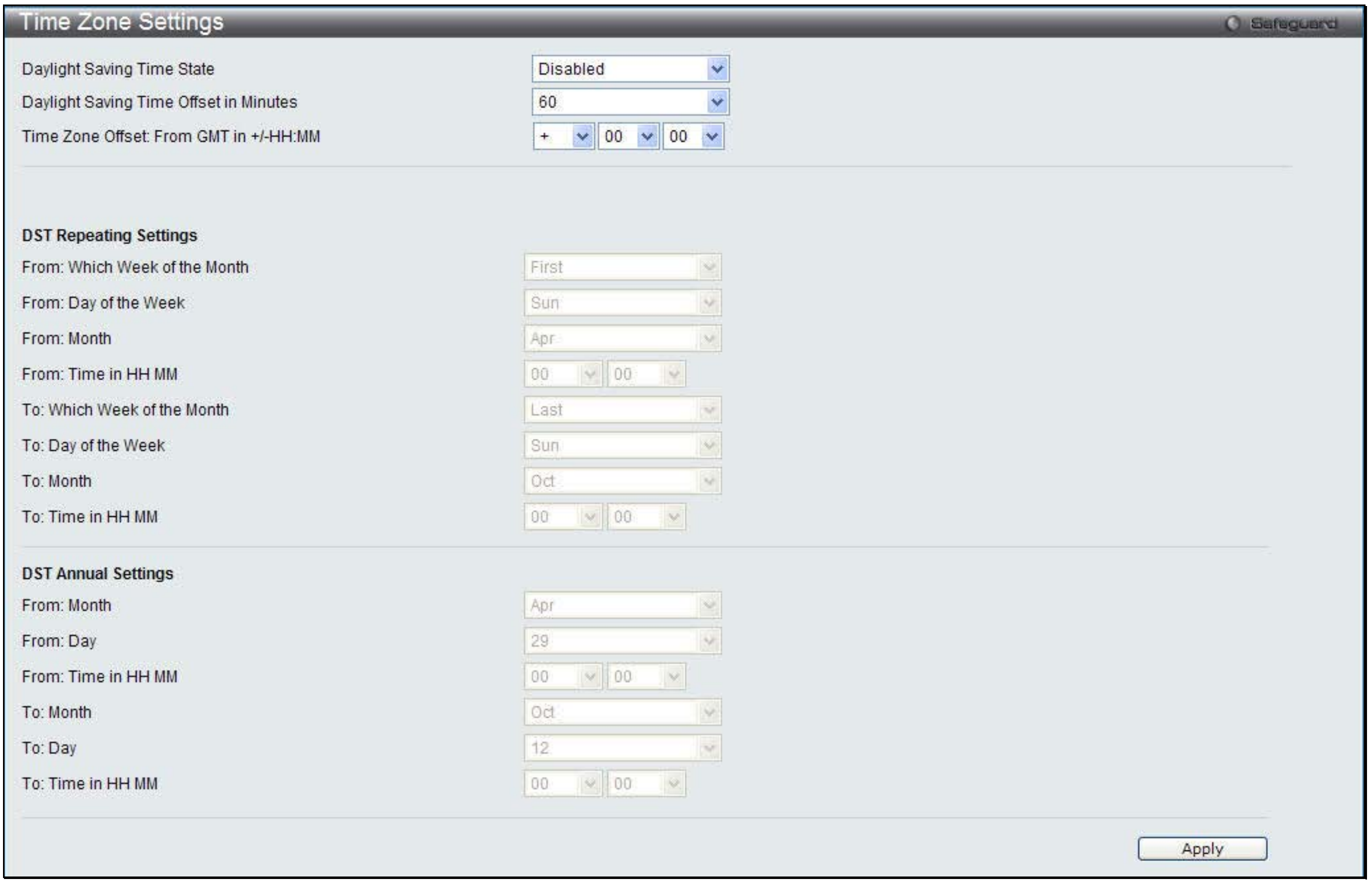
Parameter	Description
SNTP State	Use this radio button to enable or disable SNTP.
Current Time	Displays the Current Time.
Time Source	Displays the time source for the system.
SNTP First Server	The IP address of the primary server from which the SNTP information will be taken.
SNTP Second Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval In Seconds (30-99999)	The interval, in seconds, between requests for updated SNTP information.

Click the **Apply** button to accept the changes made.

Time Zone Settings

Users can configure time zones and Daylight Savings Time settings for SNTP.

To view this window, click **Network Application > SNTP > Time Zone Settings** as shown below:



Daylight Saving Time State: Disabled
Daylight Saving Time Offset in Minutes: 60
Time Zone Offset: From GMT in +/-HH:MM: + 00 00

DST Repeating Settings

From: Which Week of the Month: First
From: Day of the Week: Sun
From: Month: Apr
From: Time in HH MM: 00 00
To: Which Week of the Month: Last
To: Day of the Week: Sun
To: Month: Oct
To: Time in HH MM: 00 00

DST Annual Settings

From: Month: Apr
From: Day: 29
From: Time in HH MM: 00 00
To: Month: Oct
To: Day: 12
To: Time in HH MM: 00 00

Figure 9-16 Time Zone Settings window

The fields that can be configured are described below:

Parameter	Description
Daylight Saving Time State	Use this drop-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset In Minutes	Use this drop-down menu to specify the amount of time that will constitute your local DST offset – *30*, *60*, *90*, or *120* minutes.
Time Zone Offset From GMT In +/- HH:MM	Use these drop-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

Parameter	Description
DST Repeating Settings	Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.
From: Which Week Of The Month	Enter the week of the month that DST will start.
From: Day Of Week	Enter the day of the week that DST will start on.
From: Month	Enter the month DST will start on.
From: Time In HH:MM	Enter the time of day that DST will start on.
To: Which Week Of The Month	Enter the week of the month the DST will end.
To: Day Of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.

To: Time In HH:MM	Enter the time DST will end.

Parameter	Description
DST Annual Settings	Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: Time In HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time In HH:MM	Enter the time of day that DST will end on, each year.

Click the **Apply** button to accept the changes made.

Flash File System Settings

Why use flash file system:

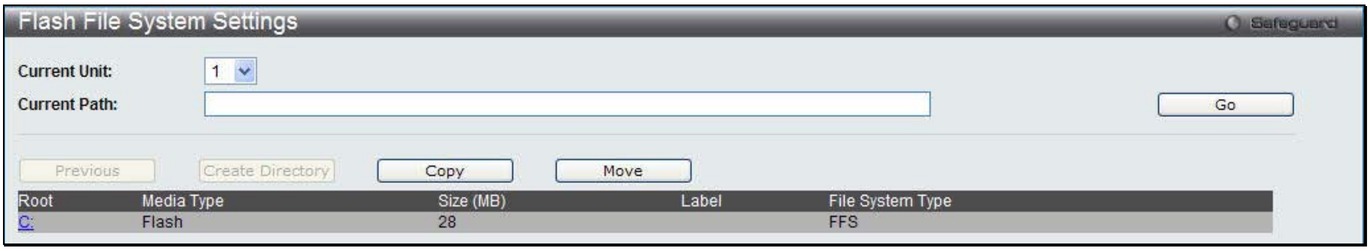
In old switch system, the firmware, configuration and log information are saved in a flash with fixed addresses and size. This means that the maximum configuration file can only be 2Mb, and even if the current configuration is only 40Kb, it will still take up 2Mb of flash storage space. The configuration file number and firmware numbers are also fixed. A compatible issue will occur in the event that the configuration file or firmware size exceeds the originally designed size.

Flash File System in our system:

The Flash File System is used to provide the user with flexible file operation on the Flash. All the firmware, configuration information and system log information are stored in the Flash as files. This means that the Flash space taken up by all the files are not fixed, it is the real file size. If the Flash space is enough, the user could download more configuration files or firmware files and use commands to display Flash file information, rename file names, and delete it. Furthermore, the user can also configure the **boot up runtime image** or the **running configuration file** if needed.

In case the file system gets corrupted, Z-modem can be used to download the backup files directly to the system.

To view this window, click **Network Application > Flash File System Settings** as shown below:



Current Unit: 1

Current Path:

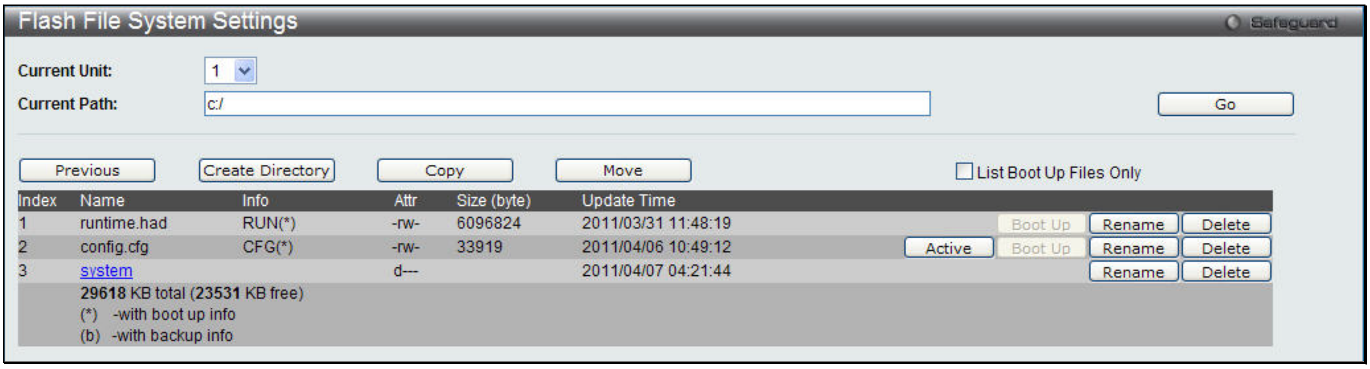
Root	Media Type	Size (MB)	Label	File System Type
C:	Flash	28		FFS

Figure 9-17 Flash File System Settings window

Enter the **Current Path** string and click the **Go** button to navigate to the path entered.

Click the C: link to navigate the C: drive

After clicking the C: link button, the following page will appear:


Flash File System Settings
Safeguard
Go
Previous
Create Directory
Copy
Move
☐ List Boot Up Files Only
Active
Boot Up
Rename
Delete

Current Unit: 1
Current Path: c:/

Index	Name	Info	Attr	Size (byte)	Update Time
1	runtime.had	RUN(*)	-rw-	6096824	2011/03/31 11:48:19
2	config.cfg	CFG(*)	-rw-	33919	2011/04/06 10:49:12
3	system		d---		2011/04/07 04:21:44

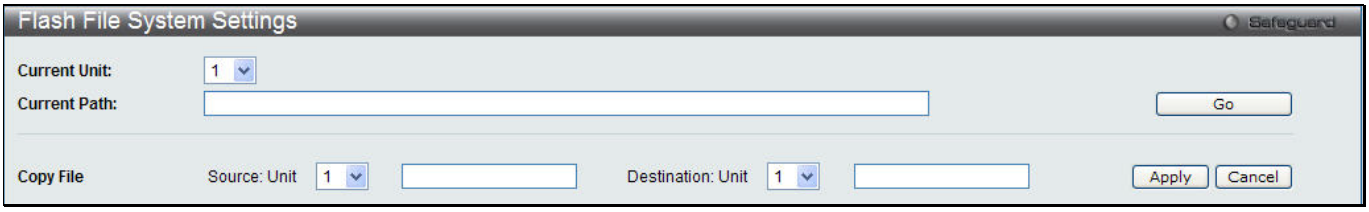
29618 KB total (**23531** KB free)
(*) -with boot up info
(b) -with backup info

Figure 9-18 Flash File System Setting – Search for Drive window

Click the **Previous** button to return to the previous page.
Click the **Create Directory** to create a new directory within the file system of the switch.
Click the **Copy** button to copy a specific file to the switch.
Click the **Move** button to move a specific file within the switch.
Tick the **List Boot Up Files Only** option to display only the boot up files.

Click the **Active** button to set a specific config file as the active runtime configuration.
Click the **Boot Up** button to set a specific runtime image as the boot up image.
Click the **Rename** button to rename a specific file's name.
Click the **Delete** button to remove a specific file from the file system.

After clicking the **Copy** button, the following page will appear:

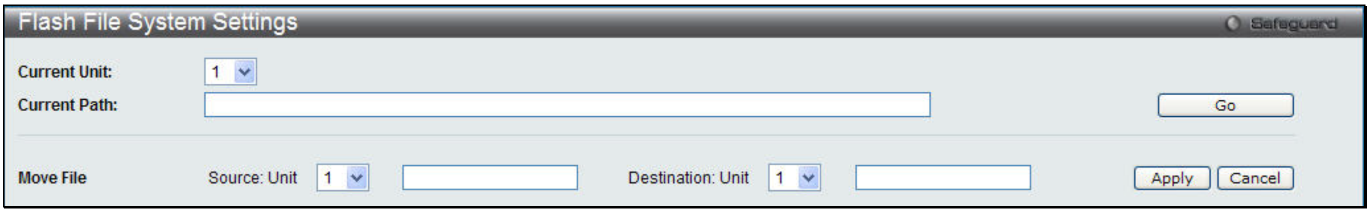

Flash File System Settings
Safeguard
Current Unit:
Current Path:
Go
Copy File
Source: Unit
Destination: Unit
Apply
Cancel

Current Unit: 1
Copy File Source: Unit 1 Destination: Unit 1

Figure 9-19 Flash File System Settings – Copy window

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path.
Click the **Apply** button to initiate the copy.
Click the **Cancel** button the discard the process.

After clicking the **Move** button, the following page will appear:


Flash File System Settings
Safeguard
Current Unit:
Current Path:
Go
Move File
Source: Unit
Destination: Unit
Apply
Cancel

Current Unit: 1
Move File Source: Unit 1 Destination: Unit 1

Figure 9-20 Flash File System Settings – Move window

When moving a file to another place, the user must enter the **Source** and **Destination** path.
Click the **Apply** button to initiate the copy.
Click the **Cancel** button the discard the process.

Chapter 10 OAM

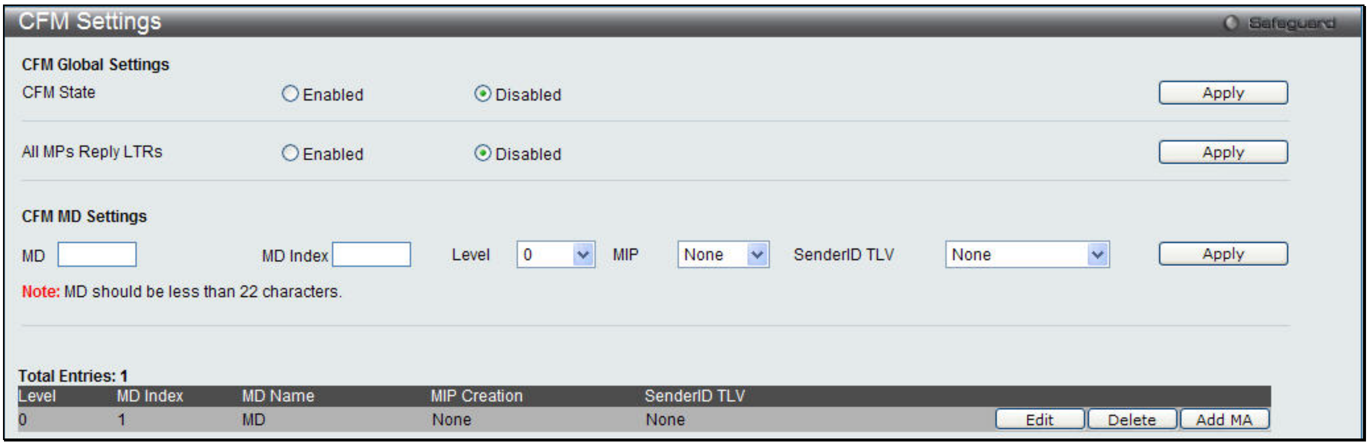
CFM (EI Mode Only)
Ethernet OAM (EI Mode Only)
DULD Settings (EI Mode Only)
Cable Diagnostics

CFM (EI Mode Only)

CFM Settings

This window is used to configure the CFM parameters.

To view this window, click **OAM > CFM > CFM Settings**, as shown below:



CFM Global Settings

CFM State ○ Enabled ● Disabled

All MPs Reply LTRs ○ Enabled ● Disabled

CFM MD Settings

MD: MD Index: Level: 0 MIP: None SenderID TLV: None

Note: MD should be less than 22 characters.

Total Entries: 1

Level	MD Index	MD Name	MIP Creation	SenderID TLV
0	1	MD	None	None

Figure 10-1 CFM Settings Window

The fields that can be configured are described below:

Parameter	Description
CFM State	Here the user can enable or disable the CFM feature.
All MPs Reply LTRs	Here the user can enable or disable all MPs to reply LTRs.
MD	Here the user can enter the maintenance domain name.
MD Index	Specifies the maintenance domain index used.
Level	Here the user can select the maintenance domain level.
MIP	This is the control creations of MIPs. *None* – Don’t create MIPs. This is the default value. *Auto* – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device. *Explicit* – MIPs can be created on any ports in this MD, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MD.
SenderID TLV	This is the control transmission of the SenderID TLV. *None* – Don’t transmit sender ID TLV. This is the default value. *Chassis* – Transmit sender ID TLV with chassis ID information. *Manage* – Transmit sender ID TLV with managed address information. *Chassis Manage* – Transmit sender ID TLV with chassis ID information and manage

	address information.

Click the **Apply** button to accept the changes made for each individual section.

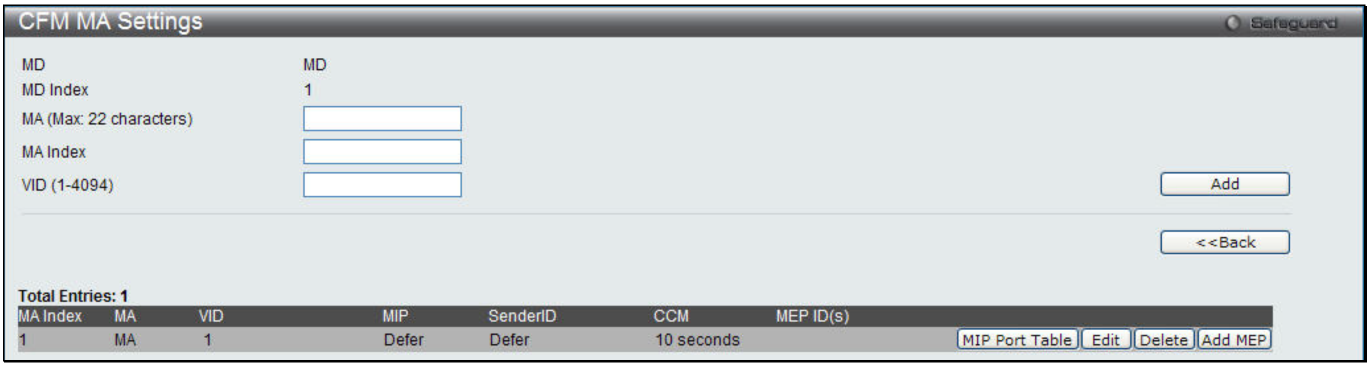
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

NOTE: The MD Name value should be less than 22 characters.

To add a maintenance association (MA), click on the **Add MA** button.

After clicking the **Add MA** button, the following page will appear:



MD: MD
MD Index: 1

Total Entries: 1

MA Index	MA	VID	MIP	SenderID	CCM	MEP ID(s)	
1	MA	1	Defer	Defer	10 seconds		MIP Port Table Edit Delete Add MEP

Figure 10-2 CFM MA Settings Window

The fields that can be configured are described below:

Parameter	**Description**
MA	Here the user can enter the maintenance association name.
MA Index	Here the user can enter the maintenance association index.
VID	VLAN Identifier. Different MA must be associated with different VLANs.

Click the **Add** button to add a new entry based on the information entered.

Click the **<<Back** button to discard the changes made and return to the previous page.

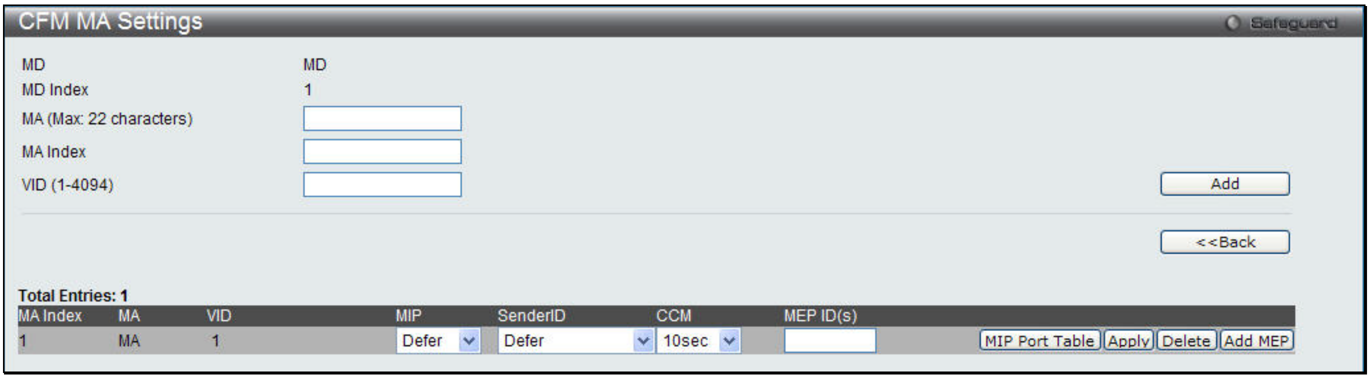
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Click the **MIP Port Table** button to view the CFM MIP Table.

Click the **Add MEP** button to add a Maintenance End Point entry.

After click in the **Edit** button the following window appears:



MD: MD
MD Index: 1

Total Entries: 1

MA Index	MA	VID	MIP	SenderID	CCM	MEP ID(s)	
1	MA	1	Defer	Defer	10sec		MIP Port Table Apply Delete Add MEP

Figure 10-3 CFM MA Settings - Edit Window

The fields that can be configured are described below:

Parameter	Description
MIP	This is the control creation of MIPs. *None* - Don’t create MIPs. *Auto* - MIPs can always be created on any ports in this MA, if that port is not configured with a MEP of that MA. *Explicit* - MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
SenderID	This is the control transmission of the sender ID TLV. *None* - Don’t transmit sender ID TLV. This is the default value. *Chassis* - Transmit sender ID TLV with chassis ID information. *Manage* - Transmit sender ID TLV with manage address information. *Chassis Manage* - Transmit sender ID TLV with chassis ID information and manage address information. *Defer* - Inherit the setting configured for the maintenance domain that this MA is associated with. This is the default value.
CCM	This is the CCM interval. *10ms* - 10 milliseconds. Not recommended. For test purpose. *100ms* - 100 milliseconds. Not recommended. For test purpose. *1sec* - One second. *10sec* - Ten seconds. This is the default value. *1min* - One minute. *10min* - Ten minutes.
MEP ID(s)	This is to specify the MEP IDs contained in the maintenance association. The range of the MEP ID is 1-8191. *Add* - Add MEP ID(s). *Delete* - Delete MEP ID(s). By default, there is no MEP ID in a newly created maintenance association.

Click the **Apply** button to accept the changes made.

After clicking the **MIP Port Table** button, the following page will appear:

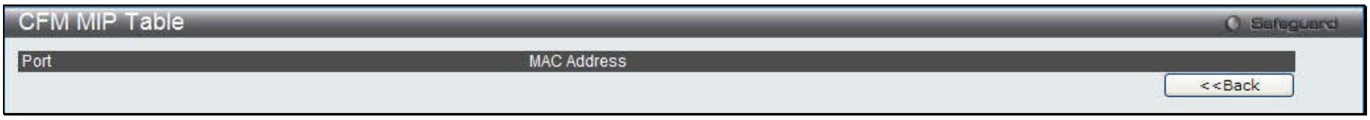
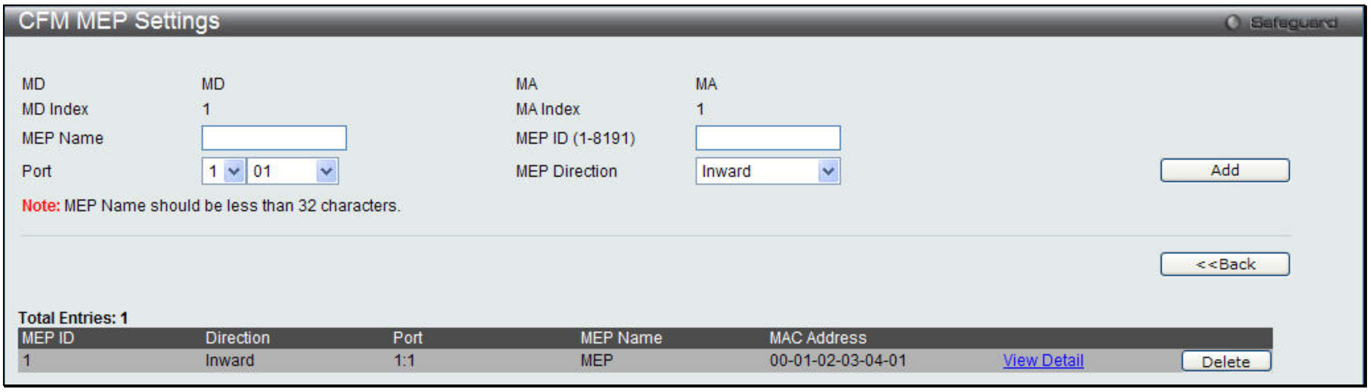


Figure 10-4 CFM MIP Port Table Window

Click the **<<Back** button to return to the previous page.

After clicking the **Add MEP** button, the following page will appear:



MD	MD	MA	MA
MD Index	1	MA Index	1
MEP Name		MEP ID (1-8191)	
Port	1 01	MEP Direction	Inward

Note: MEP Name should be less than 32 characters.

Total Entries: 1

MEP ID	Direction	Port	MEP Name	MAC Address		
1	Inward	1:1	MEP	00-01-02-03-04-01	View Detail	Delete

Figure 10-5 CFM MEP Settings (Add) Window

The fields that can be configured are described below:

Parameter	Description
MEP Name	MEP name. It is unique among all MEPs configured on the device.
MEP ID (1-8191)	MEP MEPID. It should be configured in the MA’s MEP ID list.
Port	Port number. This port should be a member of the MA’s associated VLAN.
MEP Direction	This is the MEP direction. *Inward* - Inward facing (up) MEP. *Outward* - Outward facing (down) MEP.

Click the **Add** button to add a new entry based on the information entered.

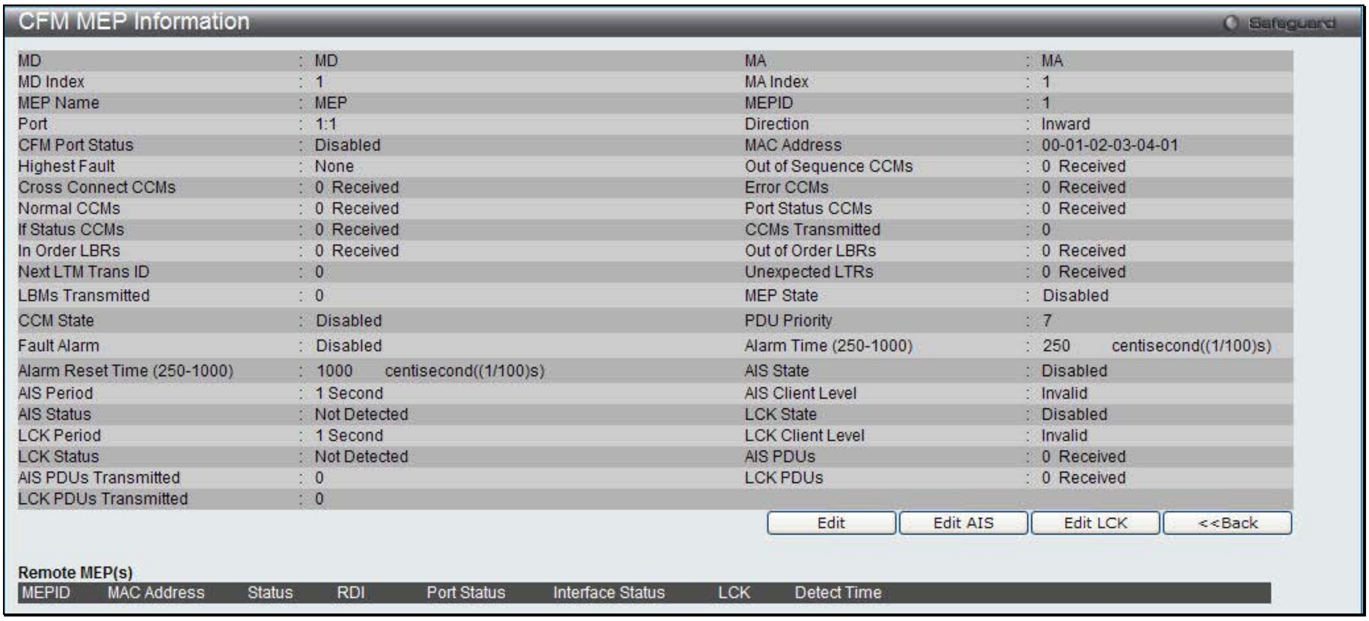
Click the **<<Back** button to discard the changes made and return to the previous page.

Click the View Detail link to view more information regarding the specific entry.

Click the **Delete** button to remove the specific entry.

NOTE: The MEP Name value should be less than 32 characters.

After clicking the View Detail link, the following page will appear:



MD	: MD	MA	: MA
MD Index	: 1	MA Index	: 1
MEP Name	: MEP	MEPID	: 1
Port	: 1:1	Direction	: Inward
CFM Port Status	: Disabled	MAC Address	: 00-01-02-03-04-01
Highest Fault	: None	Out of Sequence CCMs	: 0 Received
Cross Connect CCMs	: 0 Received	Error CCMs	: 0 Received
Normal CCMs	: 0 Received	Port Status CCMs	: 0 Received
If Status CCMs	: 0 Received	CCMs Transmitted	: 0
In Order LBRs	: 0 Received	Out of Order LBRs	: 0 Received
Next LTM Trans ID	: 0	Unexpected LTRs	: 0 Received
LBMs Transmitted	: 0	MEP State	: Disabled
CCM State	: Disabled	PDU Priority	: 7
Fault Alarm	: Disabled	Alarm Time (250-1000)	: 250 centisecond((1/100)s)
Alarm Reset Time (250-1000)	: 1000 centisecond((1/100)s)	AIS State	: Disabled
AIS Period	: 1 Second	AIS Client Level	: Invalid
AIS Status	: Not Detected	LCK State	: Disabled
LCK Period	: 1 Second	LCK Client Level	: Invalid
LCK Status	: Not Detected	AIS PDUs	: 0 Received
AIS PDUs Transmitted	: 0	LCK PDUs	: 0 Received
LCK PDUs Transmitted	: 0		

Remote MEP(s)

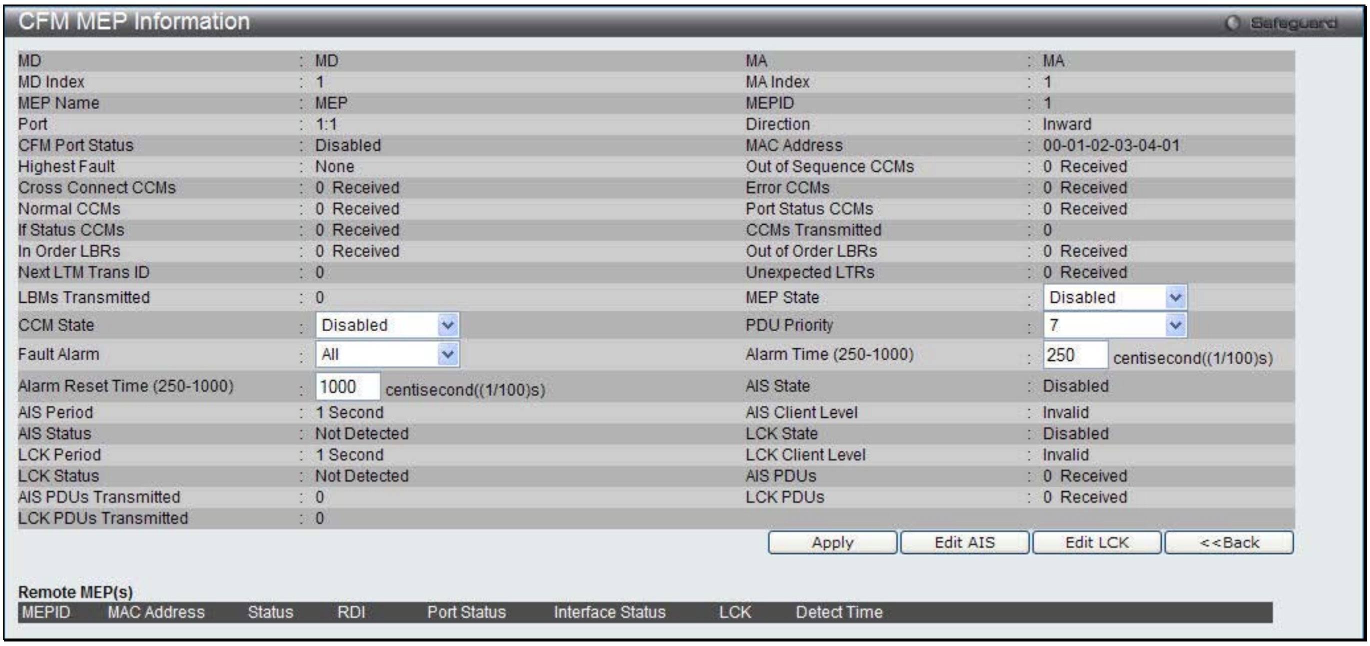
MEPID	MAC Address	Status	RDI	Port Status	Interface Status	LCK	Detect Time

Figure 10-6 CFM MEP Information Window

Click the **Edit** button to re-configure the specific entry.

Click the **<<Back** button to discard the changes made and return to the previous page.

After clicking the **Edit** button, the following page will appear:



MD	: MD	MA	: MA
MD Index	: 1	MA Index	: 1
MEP Name	: MEP	MEPID	: 1
Port	: 1:1	Direction	: Inward
CFM Port Status	: Disabled	MAC Address	: 00-01-02-03-04-01
Highest Fault	: None	Out of Sequence CCMs	: 0 Received
Cross Connect CCMs	: 0 Received	Error CCMs	: 0 Received
Normal CCMs	: 0 Received	Port Status CCMs	: 0 Received
If Status CCMs	: 0 Received	CCMs Transmitted	: 0
In Order LBRs	: 0 Received	Out of Order LBRs	: 0 Received
Next LTM Trans ID	: 0	Unexpected LTRs	: 0 Received
LBMs Transmitted	: 0	MEP State	: Disabled
CCM State	: Disabled	PDU Priority	: 7
Fault Alarm	: All	Alarm Time (250-1000)	: 250 centisecond((1/100)s)
Alarm Reset Time (250-1000)	: 1000 centisecond((1/100)s)	AIS State	: Disabled
AIS Period	: 1 Second	AIS Client Level	: Invalid
AIS Status	: Not Detected	LCK State	: Disabled
LCK Period	: 1 Second	LCK Client Level	: Invalid
LCK Status	: Not Detected	AIS PDUs	: 0 Received
AIS PDUs Transmitted	: 0	LCK PDUs	: 0 Received
LCK PDUs Transmitted	: 0		

Remote MEP(s)

MEPID	MAC Address	Status	RDI	Port Status	Interface Status	LCK	Detect Time

Figure 10-7 CFM MEP Information - Edit Window

The fields that can be configured are described below:

Parameter	Description
MEP State	This is the MEP administrative state. *Enable* - MEP is enabled. *Disable* - MEP is disabled. This is the default value.
CCM State	This is the CCM transmission state. *Enable* - CCM transmission enabled. *Disable* - CCM transmission disabled. This is the default value.
PDU Priority	The 802.1p priority is set in the CCMs and the LTMs messages transmitted by the MEP. The default value is 7.
Fault Alarm	This is the control types of the fault alarms sent by the MEP. *All* - All types of fault alarms will be sent. *MAC Status* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Error” are sent. *Remote CCM* - Only the fault alarms whose priority is equal to or higher than “Some Remote MEP Down” are sent. *Errors CCM* - Only the fault alarms whose priority is equal to or higher than “Error CCM Received” are sent. *Xcon CCM* - Only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” are sent. *None* - No fault alarm is sent. This is the default value.
Alarm Time	This is the time that a defect must exceed before the fault alarm can be sent. The unit is in centiseconds, the range is 250-1000. The default value is 250.
Alarm Reset Time	This is the dormant duration time before a defect is triggered before the fault can be re-alarmed. The unit is in centiseconds, the range is 250-1000. The default value is 1000

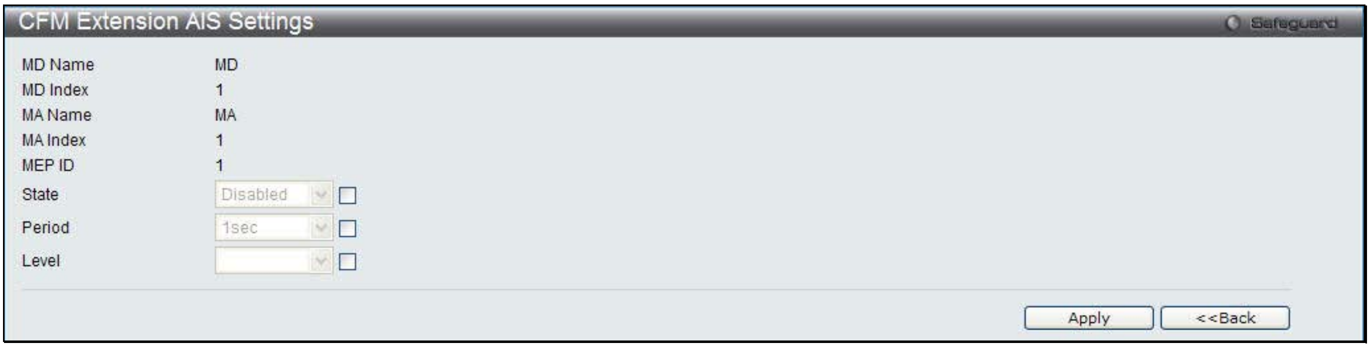
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

Click the **Edit AIS** button to configure the AIS settings.

Click the **Edit LCK** button to configure the LCK settings.

After clicking the **Edit AIS** button, the following window will appear:



CFM Extension AIS Settings

MD Name MD
MD Index 1
MA Name MA
MA Index 1
MEP ID 1
State Disabled ☐
Period 1sec ☐
Level ☐

Figure 10-8 CFM Extension AIS Window

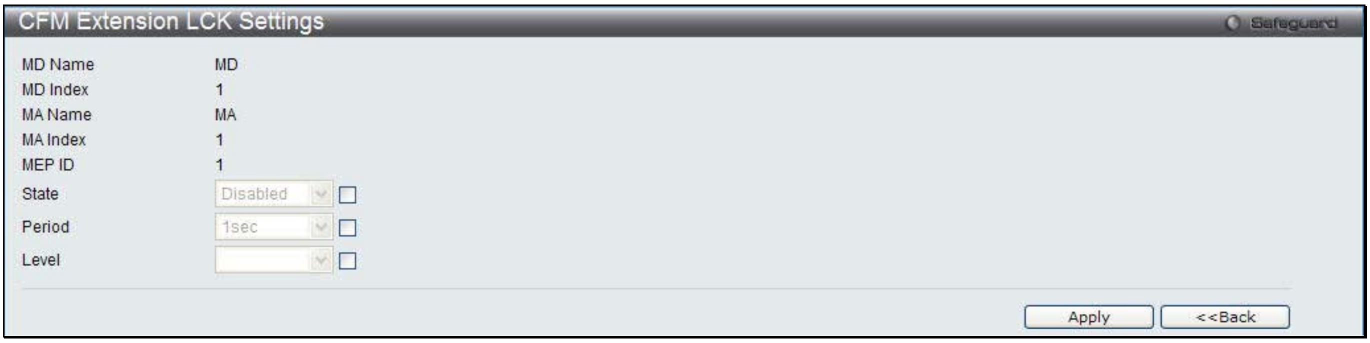
The fields that can be configured are described below:

Parameter	Description
State	Specifies to *enable* or *disable* the AIS function.
Period	The transmitting interval of AIS PDU. The default period is 1 second. Options to choose from are: *1sec* - Specifies that the transmitting interval will be set to 1 second. *1min* - Specifies that the transmitting interval will be set to 1 minute.
Level	The client level ID to which the MEP sends AIS PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between *0-7*.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

After click the **Edit LCK** button, the following window will appear:



CFM Extension LCK Settings

MD Name MD
MD Index 1
MA Name MA
MA Index 1
MEP ID 1
State Disabled ☐
Period 1sec ☐
Level ☐

Figure 10-9 CFM Extension LCK Settings Window

The fields that can be configured are described below:

Parameter	Description
State	Specifies to *enable* or *disable* the LCK function.
Period	The transmitting interval of LCK PDU. The default period is 1 second. Options to choose from are: *1sec* - Specifies that the transmitting interval will be set to 1 second. *1min* - Specifies that the transmitting interval will be set to 1 minute.
Level	The client level ID to which the MEP sends LCK PDU. The default client MD level is MD level at which the most immediate client layer MIPs and MEPs exist. Options to choose from are values between *0-7*.

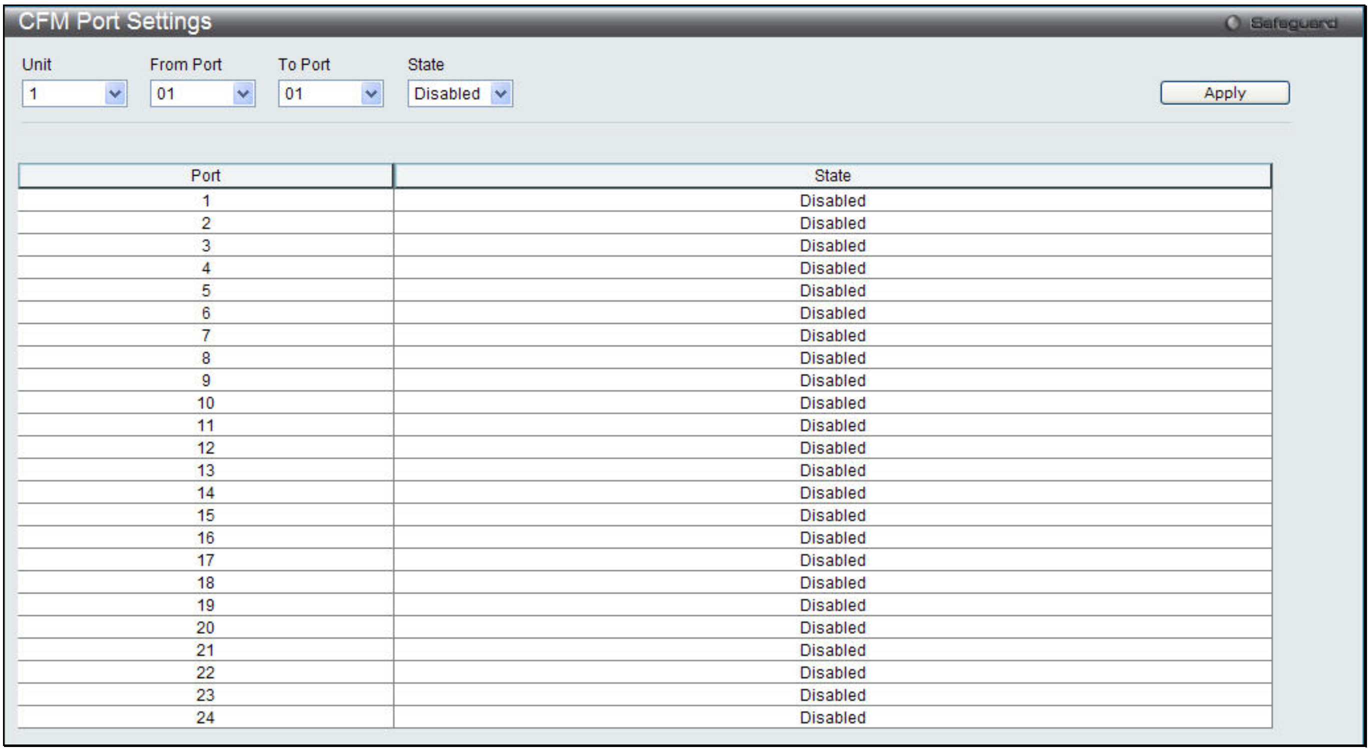
Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

CFM Port Settings

This window is used to enable or disable the CFM function on a per-port basis.

To view this window, click **OAM > CFM > CFM Port Settings**, as shown below:



Unit: 1
From Port: 01
To Port: 01
State: Disabled

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

Figure 10-10 CFM Port Settings Window

The fields that can be configured are described below:

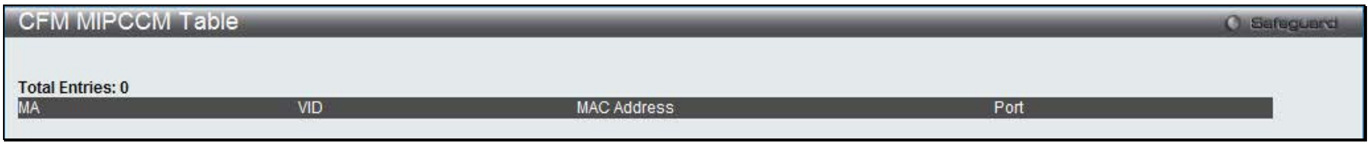
Parameter	Description
Unit	Specifies the unit's ID used.
From Port / To Port	Use the drop-down menus to select a range of ports to be configuration.
State	Use the drop-down menu to enable or disable the state of specific port regarding the CFM configuration.

Click the **Apply** button to accept the changes made.

CFM MIPCCM Table

This window is used to show the MIP CCM database entries.

To view this window, click **OAM > CFM > CFM MIPCCM Table**, as shown below:



Total Entries: 0

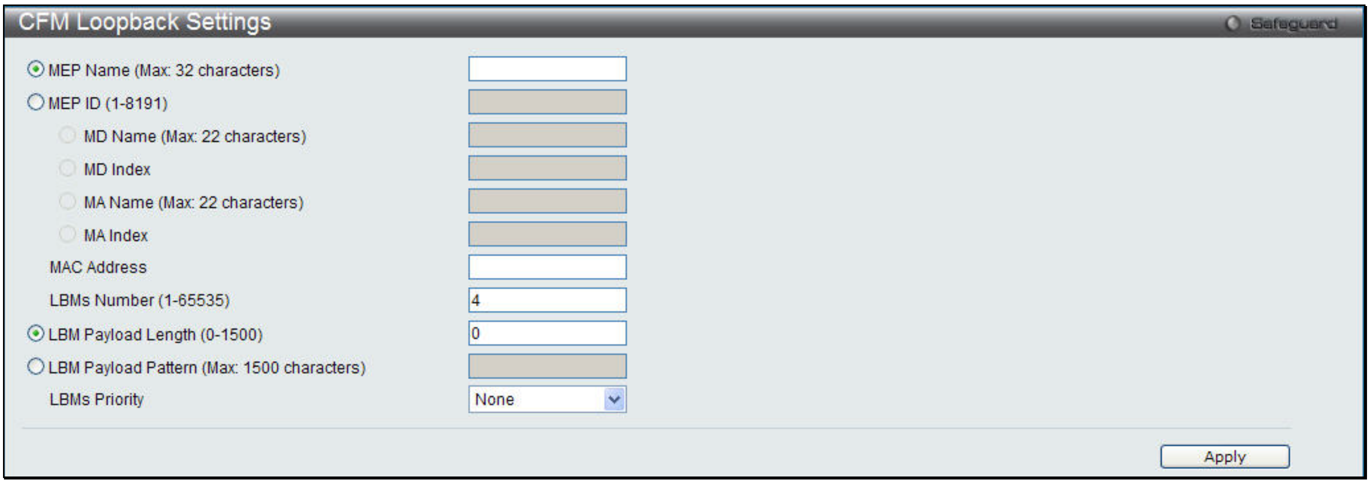
MA	VID	MAC Address	Port

Figure 10-11 CFM MIPCCM Table Window

CFM Loopback Settings

This window is used to start a CFM loopback test.

To view this window, click **OAM > CFM > CFM Loopback Settings**, as shown below:



● MEP Name (Max: 32 characters)

○ MEP ID (1-8191)

LBMs Number (1-65535): 4

● LBM Payload Length (0-1500): 0

○ LBM Payload Pattern (Max: 1500 characters)

LBMs Priority: None

Figure 10-12 CFM Loopback Settings Window

The fields that can be configured are described below:

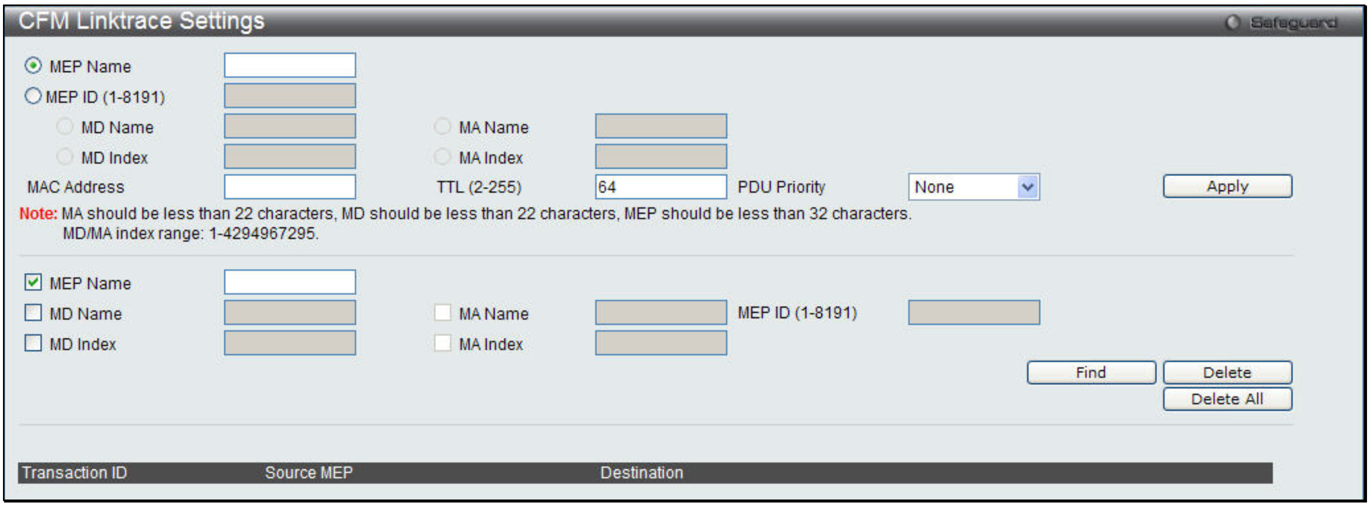
Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID (1-8191)	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.
MAC Address	Enter the destination MAC address used here.
LBMs Number (1-65535)	Number of LBMs to be sent. The default value is 4.
LBM Payload Length (0-1500)	The payload length of LBM to be sent. The default is 0.
LBM Payload Pattern	An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included.
LBMs Priority	The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.

Click the **Apply** button to accept the changes made.

CFM Linktrace Settings

This window is used to issue a CFM link track message, display or delete the link trace responses.

To view this window, click **OAM > CFM > CFM Linktrace Settings**, as shown below:


CFM Linktrace Settings
Safeguard
● MEP Name
○ MEP ID (1-8191)
○ MD Name
○ MD Index
○ MA Name
○ MA Index
MAC Address
TTL (2-255)
PDU Priority
Apply
☑ MEP Name
☐ MD Name
☐ MD Index
☐ MA Name
☐ MA Index
MEP ID (1-8191)
Find
Delete
Delete All
Transaction ID
Source MEP
Destination

TTL (2-255): 64

PDU Priority: None

Note: MA should be less than 22 characters, MD should be less than 22 characters, MEP should be less than 32 characters.
MD/MA index range: 1-4294967295.

Figure 10-13 CFM Linktrace Settings Window

The fields that can be configured are described below:

Parameter	Description
MEP Name	Select and enter the Maintenance End Point name used.
MEP ID (1-8191)	Select and enter the Maintenance End Point ID used.
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.
MA Index	Select and enter the Maintenance Association index used.
MAC Address	Here the user can enter the destination MAC address.
TTL (2-255)	Link-trace message TTL value. The default value is 64.
PDU Priority	The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.

Click the **Apply** button to accept the changes made.

Click the **Find** button to locate a specific entry based on the information entered.

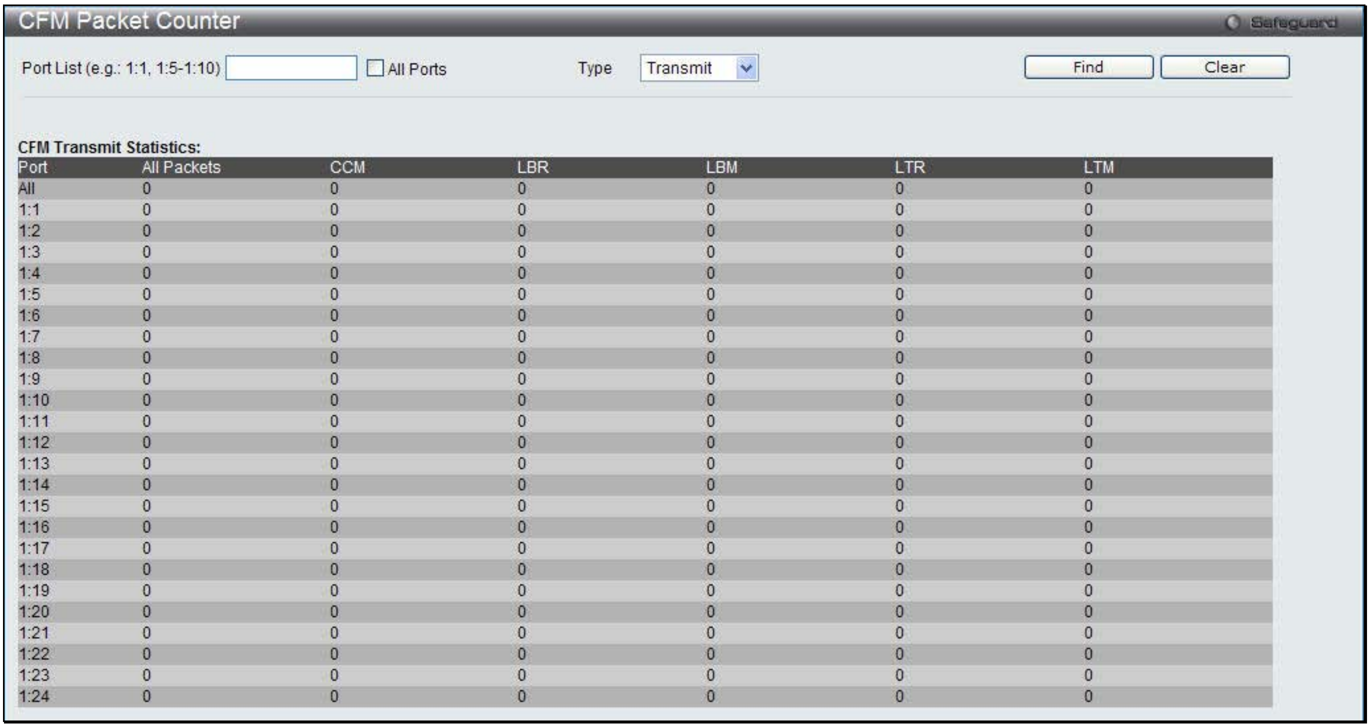
Click the **Delete** button to remove the specific entry based on the information entered.

Click the **Delete All** button to remove all the entries listed.

CFM Packet Counter

This window is used to show the CFM packet’s RX/TX counters.

To view this window, click **OAM > CFM > CFM Packet Counter**, as shown below:



CFM Transmit Statistics:

Port	All Packets	CCM	LBR	LBM	LTR	LTM
All	0	0	0	0	0	0
1:1	0	0	0	0	0	0
1:2	0	0	0	0	0	0
1:3	0	0	0	0	0	0
1:4	0	0	0	0	0	0
1:5	0	0	0	0	0	0
1:6	0	0	0	0	0	0
1:7	0	0	0	0	0	0
1:8	0	0	0	0	0	0
1:9	0	0	0	0	0	0
1:10	0	0	0	0	0	0
1:11	0	0	0	0	0	0
1:12	0	0	0	0	0	0
1:13	0	0	0	0	0	0
1:14	0	0	0	0	0	0
1:15	0	0	0	0	0	0
1:16	0	0	0	0	0	0
1:17	0	0	0	0	0	0
1:18	0	0	0	0	0	0
1:19	0	0	0	0	0	0
1:20	0	0	0	0	0	0
1:21	0	0	0	0	0	0
1:22	0	0	0	0	0	0
1:23	0	0	0	0	0	0
1:24	0	0	0	0	0	0

Figure 10-14 CFM Packet Counter Window

The fields that can be configured are described below:

Parameter	Description
Port List	Enter a list of ports to be displayed. Tick the **All Ports** check box to display all ports.
Type	*Transmit* – Selecting this option will display all the CFM packets transmitted. *Receive* – Selecting this option will display all the CFM packets received. *CCM* – Selecting this option will display all the CFM packets transmitted and received.

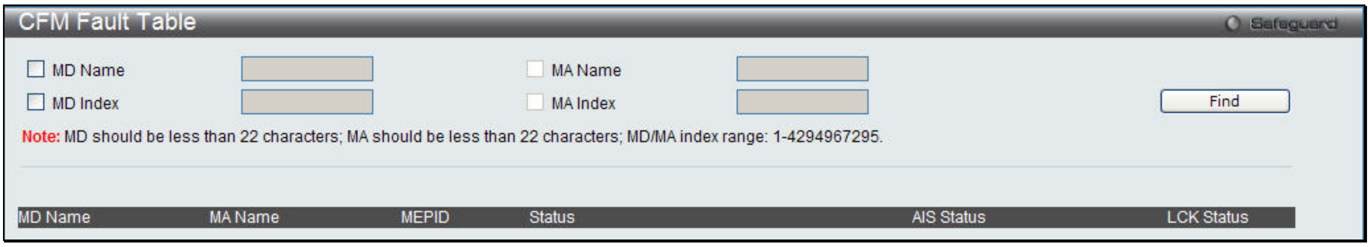
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information entered in the fields.

CFM Fault Table

This window is used to show the MEPs that have faults.

To view this window, click **OAM > CFM > CFM Fault Table**, as shown below:



Note: MD should be less than 22 characters; MA should be less than 22 characters; MD/MA index range: 1-4294967295.

MD Name	MA Name	MEPID	Status	AIS Status	LCK Status

Figure 10-15 CFM Fault Table Window

The fields that can be configured are described below:

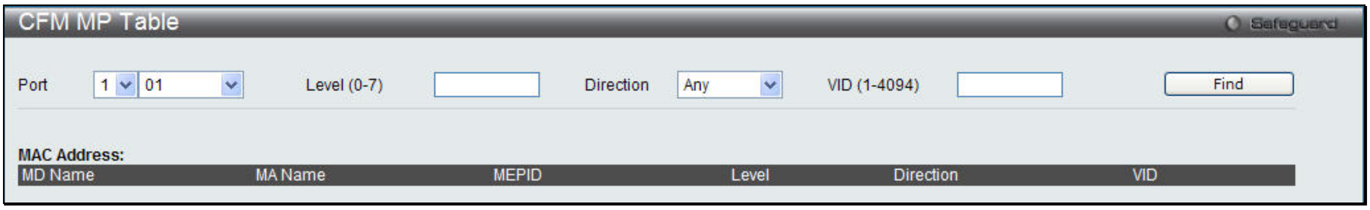
Parameter	Description
MD Name	Select and enter the Maintenance Domain name used.
MD Index	Select and enter the Maintenance Domain index used.
MA Name	Select and enter the Maintenance Association name used.

MA Index	Select and enter the Maintenance Association index used.

Click the **Find** button to locate a specific entry based on the information entered.

CFM MP Table

To view this window, click **OAM > CFM > CFM MP Table**, as shown below:



Port 1 01

Level (0-7)

Direction Any

VID (1-4094)

MAC Address:

Figure 10-16 CFM MP Table Window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the unit ID and the port number to view.
Level (0-7)	Enter the level to view.
Direction	Use the drop-down menu to select the direction to view. *Inward* - Inward facing (up) MP. *Outward* - Outward facing (down) MP.
VID (1-4094)	Enter the VID to view.

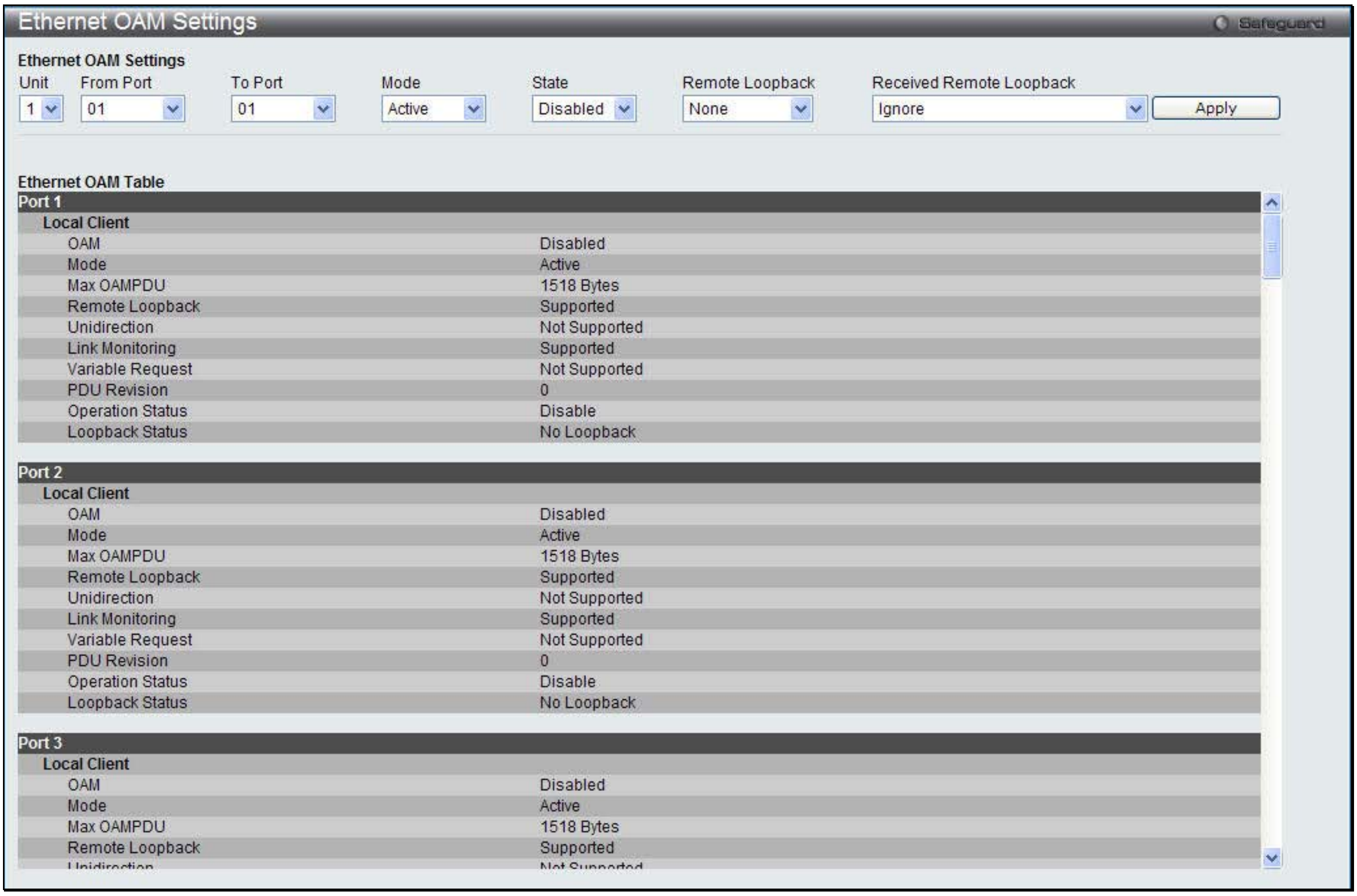
Click the **Find** button to locate a specific entry based on the information entered.

Ethernet OAM (EI Mode Only)

Ethernet OAM Settings

This window is used to configure the Ethernet OAM settings.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Settings**, as shown below:



Ethernet OAM Settings

Unit: 1
From Port: 01
To Port: 01
Mode: Active
State: Disabled
Remote Loopback: None
Received Remote Loopback: Ignore

Ethernet OAM Table

Port 1	
Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Supported
Unidirection	Not Supported
Link Monitoring	Supported
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disable
Loopback Status	No Loopback
Port 2	
Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Supported
Unidirection	Not Supported
Link Monitoring	Supported
Variable Request	Not Supported
PDU Revision	0
Operation Status	Disable
Loopback Status	No Loopback
Port 3	
Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Supported
Unidirection	Not Supported

Figure 10-17 Ethernet OAM Settings window

The fields that can be configured are described below:

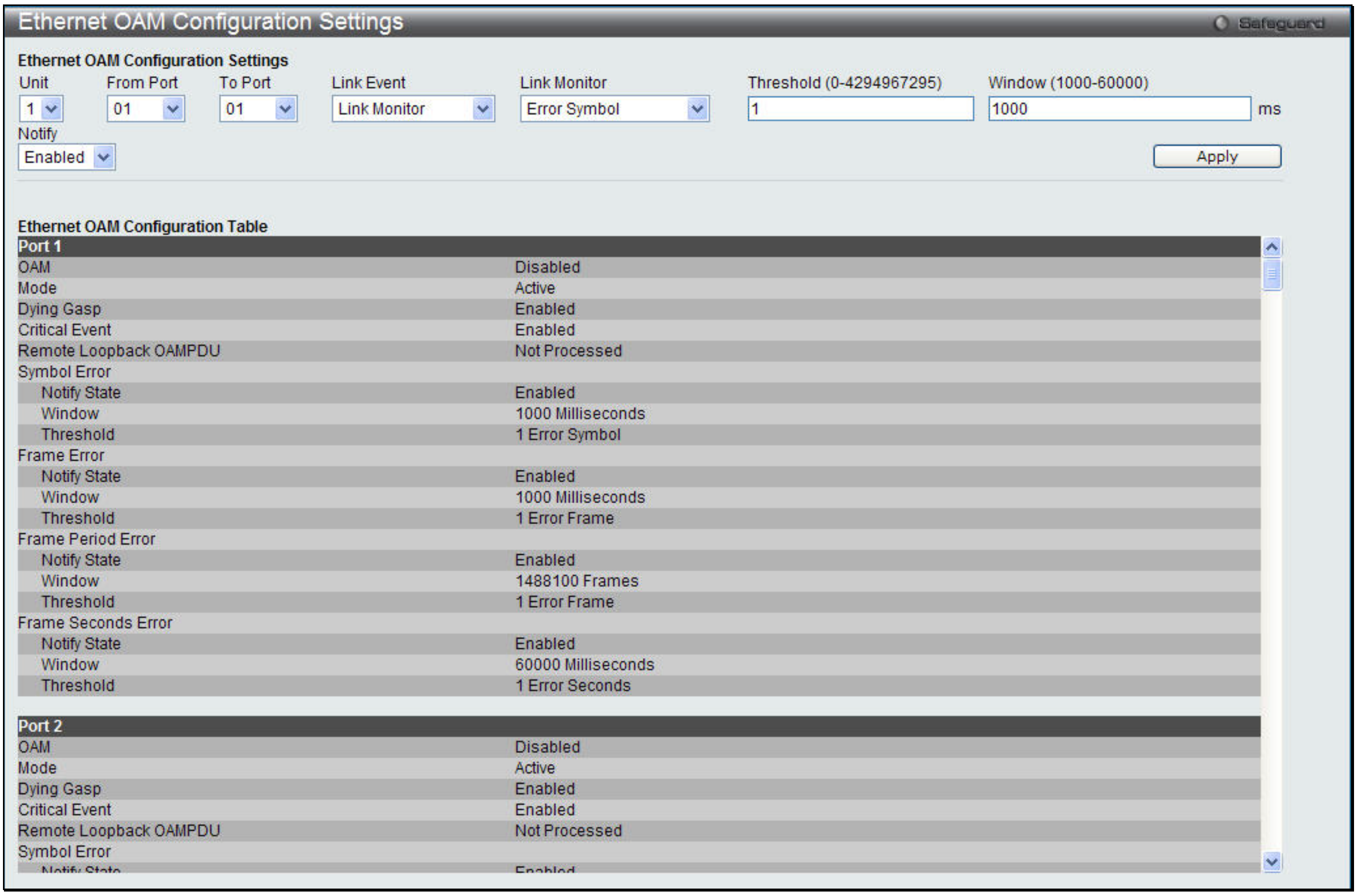
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports you wish to configure.
Mode	Use the drop-down menu to select to operate in either *Active* or *Passive*. The default mode is Active.
State	Use the drop-down menu to enable or disable the OAM function.
Remote Loopback	Use the drop-down menu to select Ethernet OAM remote loopback. *None* – Select to disable the remote loopback. *Start* – Select to request the peer to change to the remote loopback mode. *Stop* - Select to request the peer to change to the normal operation mode.
Received Remote Loopback	Use the drop-down menu to configure the client to process or to ignore the received Ethernet OAM remote loopback command. *Process* – Select to process the received Ethernet OAM remote loopback command. *Ignore* - Select to ignore the received Ethernet OAM remote loopback command.

Click the **Apply** button to accept the changes made.

Ethernet OAM Configuration Settings

This window is used to configure Ethernet OAM configuration settings.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Configuration Settings**, as shown below:



Ethernet OAM Configuration Settings

Unit	From Port	To Port	Link Event	Link Monitor	Threshold (0-4294967295)	Window (1000-60000)
1	01	01	Link Monitor	Error Symbol	1	1000 ms

Notify: Enabled

Ethernet OAM Configuration Table

Port 1	
OAM	Disabled
Mode	Active
Dying Gasp	Enabled
Critical Event	Enabled
Remote Loopback OAMPDU	Not Processed
Symbol Error	
Notify State	Enabled
Window	1000 Milliseconds
Threshold	1 Error Symbol
Frame Error	
Notify State	Enabled
Window	1000 Milliseconds
Threshold	1 Error Frame
Frame Period Error	
Notify State	Enabled
Window	1488100 Frames
Threshold	1 Error Frame
Frame Seconds Error	
Notify State	Enabled
Window	60000 Milliseconds
Threshold	1 Error Seconds

Port 2	
OAM	Disabled
Mode	Active
Dying Gasp	Enabled
Critical Event	Enabled
Remote Loopback OAMPDU	Not Processed
Symbol Error	
Notify State	Enabled

Figure 10-18 Ethernet OAM Configuration Settings window

The fields that can be configured are described below:

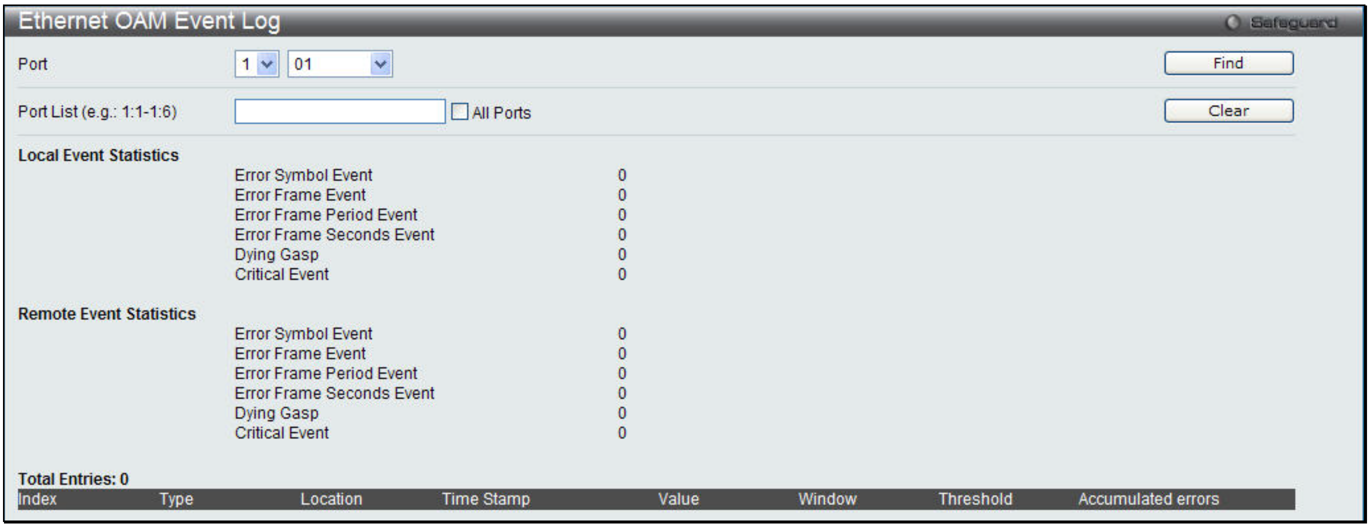
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports you wish to configure.
Link Event	Use the drop-down menu to select the link events, *Link Monitor* or *Critical Link Event*.
Link Monitor	Use the drop-down menu to select link monitor. Available options are *Error Symbol*, *Error Frame*, *Error Frame Period*, and *Error Frame Seconds*.
Critical Link Event	Use the drop-down menu to select between *Dying Gasp* and *Critical Event*.
Threshold (0-4294967295)	Enter the number of error frame or symbol in the period is required to be equal to or greater than in order for the event to be generated.
Window (1000-6000)	Enter the period of error frame or symbol in milliseconds summary event.

Click the **Apply** button to accept the changes made for each individual section.

Ethernet OAM Event Log

The window is used to show ports Ethernet OAM event log information.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Event Log**, as shown below:


Ethernet OAM Event Log
Safeguard
Port
1
01
Find
Port List (e.g.: 1:1-1:6)
☐ All Ports
Clear
Index
Type
Location
Time Stamp
Value
Window
Threshold
Accumulated errors

Local Event Statistics

Error Symbol Event	0
Error Frame Event	0
Error Frame Period Event	0
Error Frame Seconds Event	0
Dying Gasp	0
Critical Event	0

Remote Event Statistics

Error Symbol Event	0
Error Frame Event	0
Error Frame Period Event	0
Error Frame Seconds Event	0
Dying Gasp	0
Critical Event	0

Total Entries: 0

Figure 10-19 Ethernet OAM Event Log window

The fields that can be configured are described below:

Parameter	Description
Port	Use the drop-down menu to select the unit ID and the port number to view.
Port List	Enter a list of ports. Tick the **All Ports** check box to select all ports.

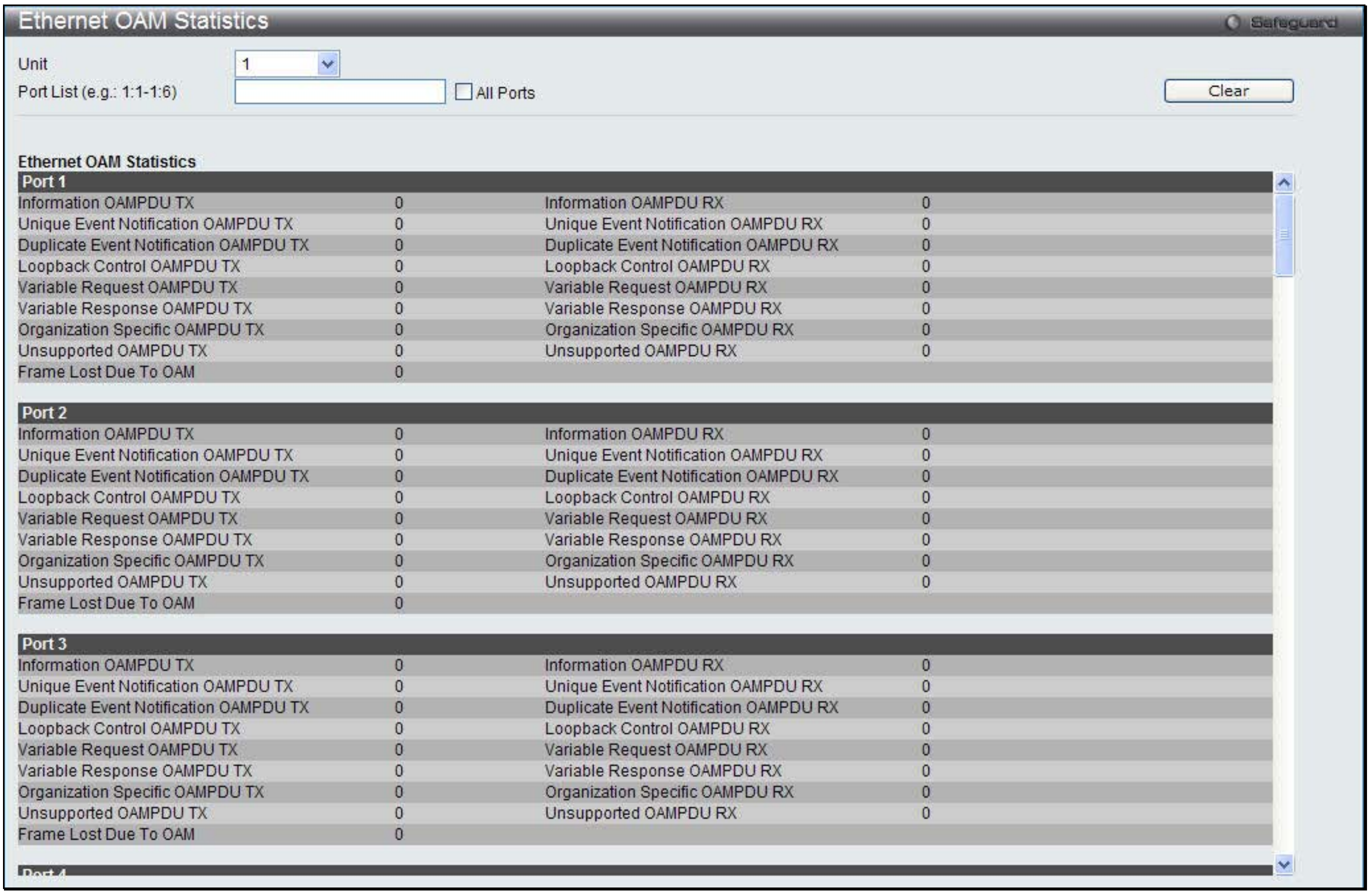
Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear** button to clear all the information entered in the fields.

Ethernet OAM Statistics

The window is used to show ports Ethernet OAM statistics information.

To view this window, click **OAM > Ethernet OAM > Ethernet OAM Statistics**, as shown below:



Unit: 1

Port List (e.g.: 1:1-1:6):

☐ All Ports

Ethernet OAM Statistics

Port 1

Information OAMPDU TX	0	Information OAMPDU RX	0
Unique Event Notification OAMPDU TX	0	Unique Event Notification OAMPDU RX	0
Duplicate Event Notification OAMPDU TX	0	Duplicate Event Notification OAMPDU RX	0
Loopback Control OAMPDU TX	0	Loopback Control OAMPDU RX	0
Variable Request OAMPDU TX	0	Variable Request OAMPDU RX	0
Variable Response OAMPDU TX	0	Variable Response OAMPDU RX	0
Organization Specific OAMPDU TX	0	Organization Specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame Lost Due To OAM	0		

Port 2

Information OAMPDU TX	0	Information OAMPDU RX	0
Unique Event Notification OAMPDU TX	0	Unique Event Notification OAMPDU RX	0
Duplicate Event Notification OAMPDU TX	0	Duplicate Event Notification OAMPDU RX	0
Loopback Control OAMPDU TX	0	Loopback Control OAMPDU RX	0
Variable Request OAMPDU TX	0	Variable Request OAMPDU RX	0
Variable Response OAMPDU TX	0	Variable Response OAMPDU RX	0
Organization Specific OAMPDU TX	0	Organization Specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame Lost Due To OAM	0		

Port 3

Information OAMPDU TX	0	Information OAMPDU RX	0
Unique Event Notification OAMPDU TX	0	Unique Event Notification OAMPDU RX	0
Duplicate Event Notification OAMPDU TX	0	Duplicate Event Notification OAMPDU RX	0
Loopback Control OAMPDU TX	0	Loopback Control OAMPDU RX	0
Variable Request OAMPDU TX	0	Variable Request OAMPDU RX	0
Variable Response OAMPDU TX	0	Variable Response OAMPDU RX	0
Organization Specific OAMPDU TX	0	Organization Specific OAMPDU RX	0
Unsupported OAMPDU TX	0	Unsupported OAMPDU RX	0
Frame Lost Due To OAM	0		

Figure 10-20 Ethernet OAM Statistics window

The fields that can be configured are described below:

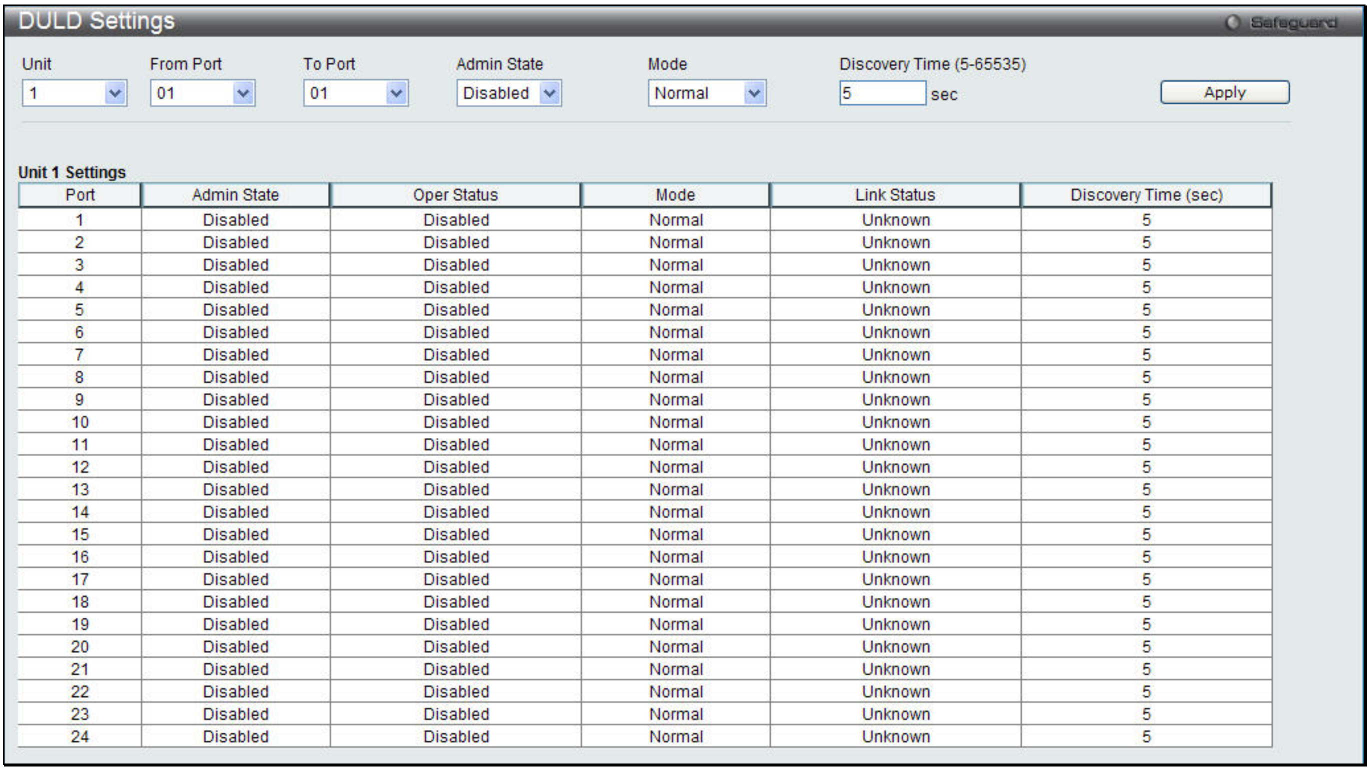
Parameter	Description
Port	Use the drop-down menu to select the unit ID and the port number to view.
Port List	Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click the **Clear** button to clear all the information entered in the fields.

DULD Settings (EI Mode Only)

This window is used to configure and display the unidirectional link detection on port.

To view this window, click **OAM > DULD Settings** as shown below:



Unit: 1 | From Port: 01 | To Port: 01 | Admin State: Disabled | Mode: Normal | Discovery Time (5-65535): 5 sec

Unit 1 Settings

Port	Admin State	Oper Status	Mode	Link Status	Discovery Time (sec)
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5
7	Disabled	Disabled	Normal	Unknown	5
8	Disabled	Disabled	Normal	Unknown	5
9	Disabled	Disabled	Normal	Unknown	5
10	Disabled	Disabled	Normal	Unknown	5
11	Disabled	Disabled	Normal	Unknown	5
12	Disabled	Disabled	Normal	Unknown	5
13	Disabled	Disabled	Normal	Unknown	5
14	Disabled	Disabled	Normal	Unknown	5
15	Disabled	Disabled	Normal	Unknown	5
16	Disabled	Disabled	Normal	Unknown	5
17	Disabled	Disabled	Normal	Unknown	5
18	Disabled	Disabled	Normal	Unknown	5
19	Disabled	Disabled	Normal	Unknown	5
20	Disabled	Disabled	Normal	Unknown	5
21	Disabled	Disabled	Normal	Unknown	5
22	Disabled	Disabled	Normal	Unknown	5
23	Disabled	Disabled	Normal	Unknown	5
24	Disabled	Disabled	Normal	Unknown	5

Figure 10-21 DULD Settings window

The fields that can be configured are described below:

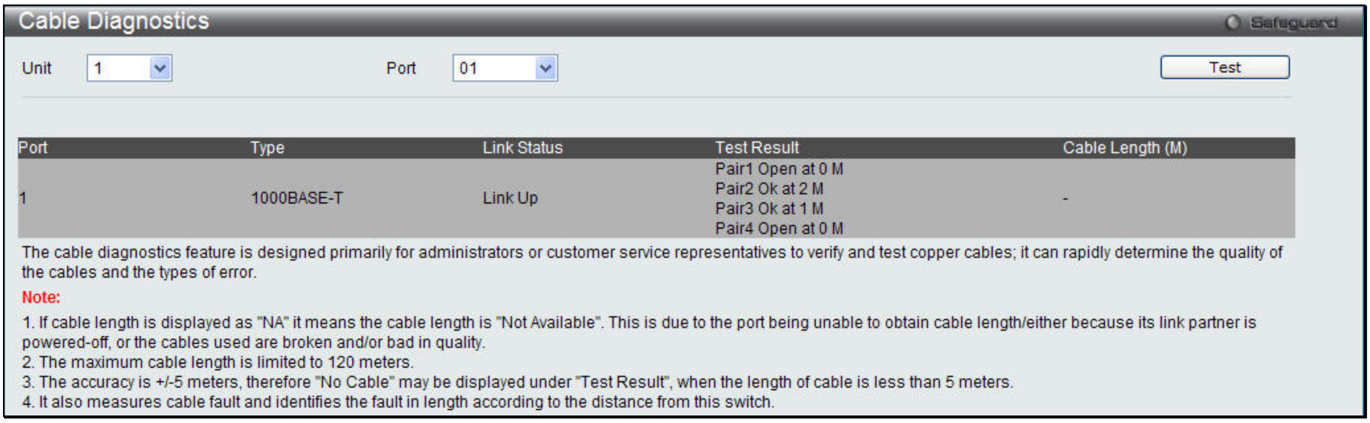
Parameter	Description
Unit	Select the unit you want to configure.
From Port / To Port	Select a range of ports you wish to configure.
Admin State	Use the drop-down menu to enable or disable the selected ports unidirectional link detection status.
Mode	Use the drop-down menu to select Mode between *Shutdown* and *Normal*. *Shutdown* – If any unidirectional link is detected, disable the port and log an event. *Normal* - Only log an event when a unidirectional link is detected.
Discovery Time (5-65535)	Enter these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start.

Click the **Apply** button to accept the changes made.

Cable Diagnostics

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

To view this window, click **OAM > Cable Diagnostics** as shown below:



Unit: 1

Port: 01

Port	Type	Link Status	Test Result	Cable Length (M)
1	1000BASE-T	Link Up	Pair1 Open at 0 M Pair2 Ok at 2 M Pair3 Ok at 1 M Pair4 Open at 0 M	-

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

Note:

1. If cable length is displayed as "NA" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link partner is powered-off, or the cables used are broken and/or bad in quality.
2. The maximum cable length is limited to 120 meters.
3. The accuracy is +/-5 meters, therefore "No Cable" may be displayed under "Test Result", when the length of cable is less than 5 meters.
4. It also measures cable fault and identifies the fault in length according to the distance from this switch.

Figure 10-22 Cable Diagnostics window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to display.
Port	Select a port you wish to display.

Click the **Test** button to view the cable diagnostics for a particular port.

NOTE: Cable diagnostic function limitations. Cable length detection is only supported on GE ports. Ports must be linked up and running at 1000M speed. Cross-talk errors detection is not supported on FE ports.

Fault messages:

- **Open** – The cable in the error pair does not have a connection at the specified position.
- **Short** – The cables in the error pair has a short problem at the specified position,
- **Crosstalk** – The cable in the error pair has a crosstalk problem at the specified position.
- **Unknow** – The diagnosis does not obtain the cable status, please try again.
- **NA** – No cable was found, maybe it's because cable is out of diagnosis specification or the quality is too bad.

Chapter 11 Monitoring

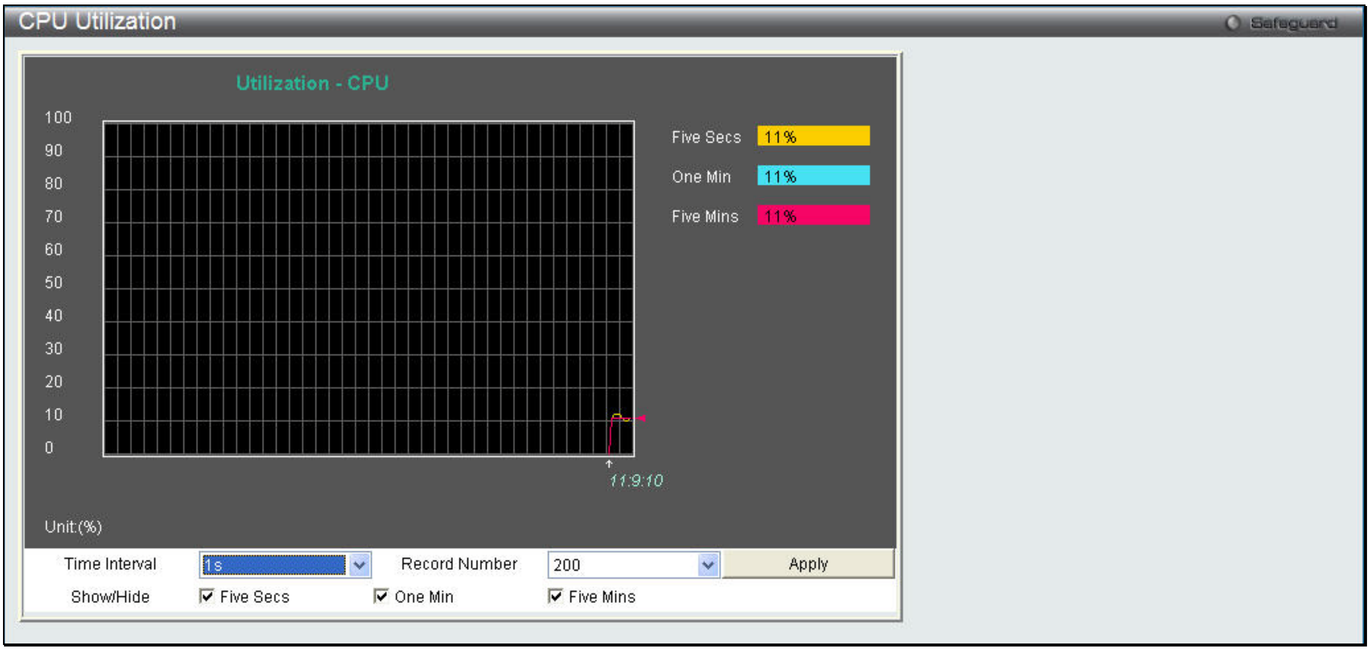
Utilization
Statistics
Mirror
sFlow (EI Mode Only)
Ping Test
Trace Route
Peripheral

Utilization

CPU Utilization

Users can display the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Monitoring > Utilization > CPU Utilization** as shown below:



Five Secs 11%
One Min 11%
Five Mins 11%

Time Interval 1s

Record Number 200

Show/Hide ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 11-1 CPU Utilization window

The fields that can be configured are described below:

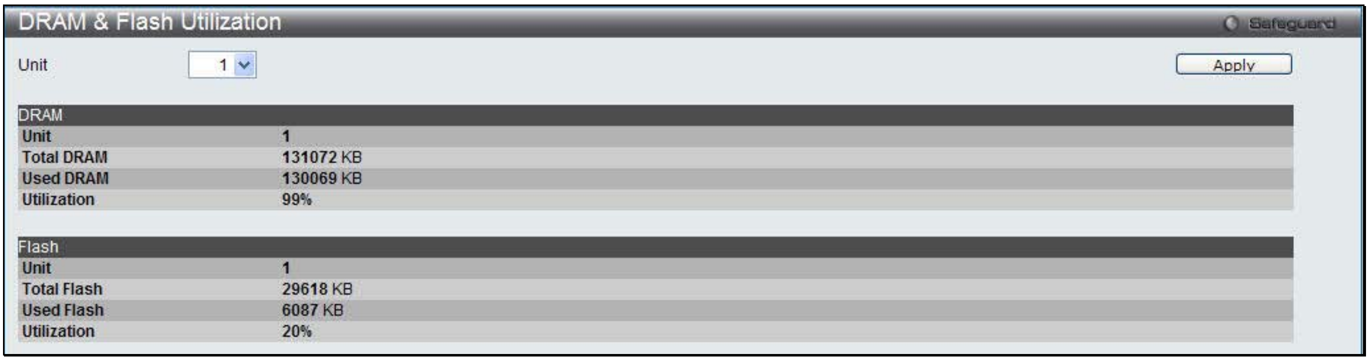
Parameter	Description
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Five Seconds, One Minute, and Five Minutes.

Click the **Apply** button to accept the changes made.

DRAM & Flash Utilization

On this page the user can view information regarding the DRAM and Flash utilization.

To view this window, click **Monitoring > Utilization > DRAM & Flash Utilization** as shown below:



DRAM & Flash Utilization

Unit 1

DRAM	
Unit	1
Total DRAM	131072 KB
Used DRAM	130069 KB
Utilization	99%

Flash	
Unit	1
Total Flash	29618 KB
Used Flash	6087 KB
Utilization	20%

Figure 11-2 DRAM & Flash Utilization window

The fields that can be configured are described below:

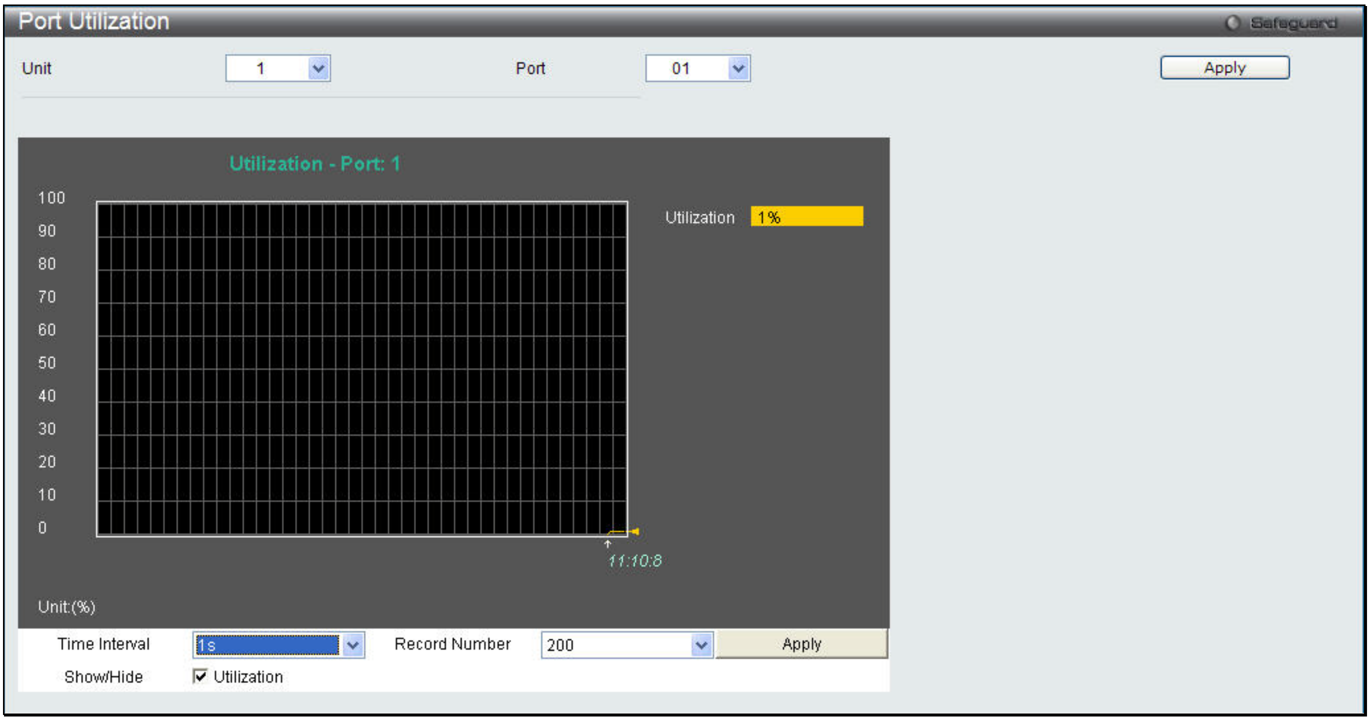
Parameter	Description
Unit	Select the unit you want to configure.

Click the **Apply** button to accept the changes made.

Port Utilization

Users can display the percentage of the total available bandwidth being used on the port.

To view this window, click **Monitoring > Utilization > Port Utilization** as shown below:



Port Utilization

Unit 1

Port 01

Utilization 1%

Time Interval 1s

Record Number 200

Show/Hide ☑ Utilization

Figure 11-3 Port Utilization window

The fields that can be configured are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The

	default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Check whether or not to display Port Util.

Click the **Apply** button to accept the changes made for each individual section.

Statistics

Port Statistics

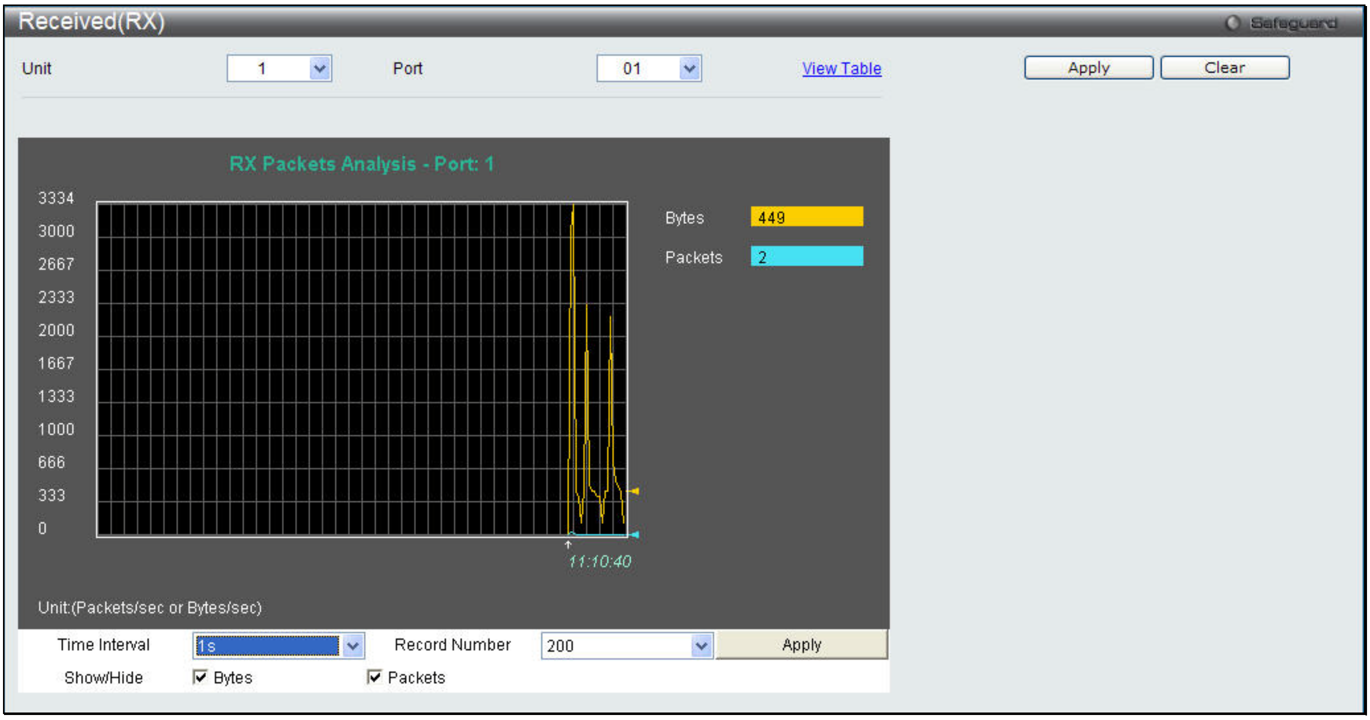
Packets

The Web manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Port Statistics > Packets > Received (RX)** as shown below:



Unit: 1

Port: 01

Bytes: 449

Packets: 2

Time Interval: 1s

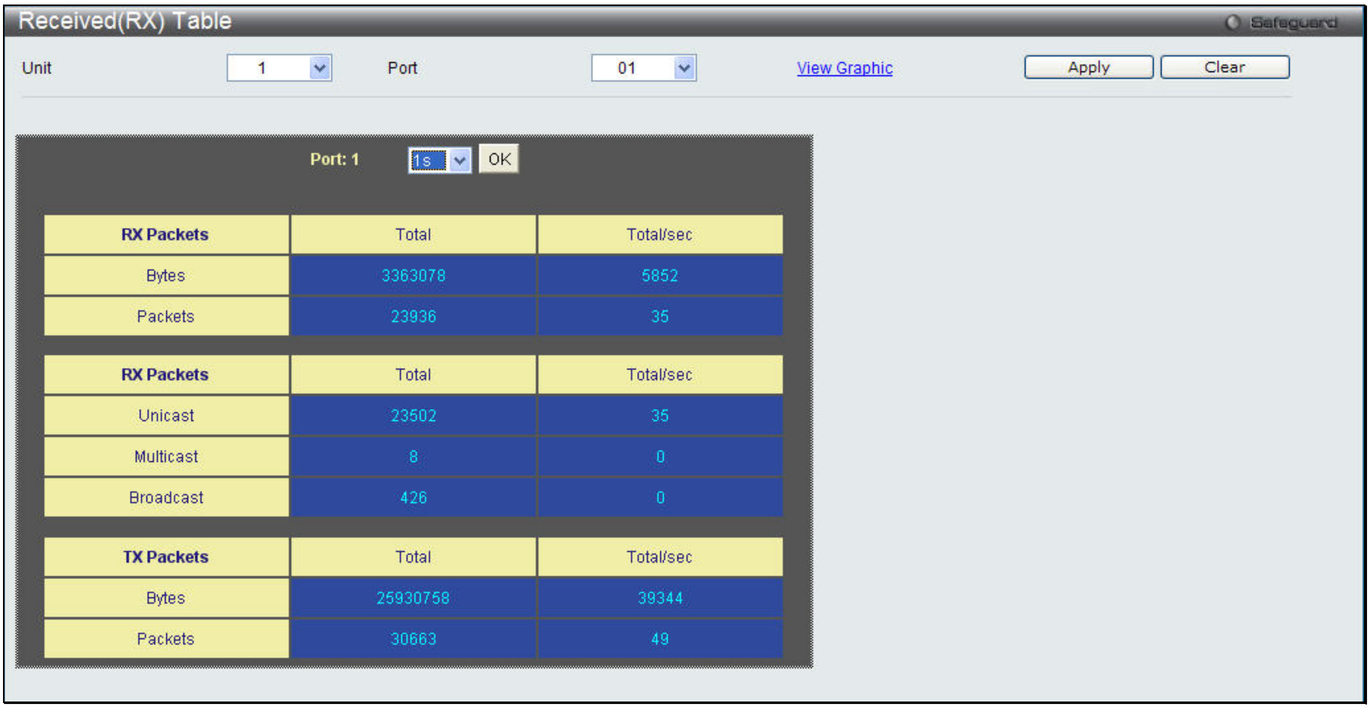
Record Number: 200

Show/Hide: ☑ Bytes ☑ Packets

Received(RX)
Safeguard
View Table
Apply
Clear
RX Packets Analysis - Port: 1
3334
3000
2667
2333
2000
1667
1333
1000
666
333
0
11:10:40
Unit:(Packets/sec or Bytes/sec)
Apply

Figure 11-4 Received (RX) window (for Bytes and Packets)

Click the View Table link to display the information in a table rather than a line graph.



Unit 1

Port 01

Port: 1 1s

RX Packets	Total	Total/sec
Bytes	3363078	5852
Packets	23936	35

RX Packets	Total	Total/sec
Unicast	23502	35
Multicast	8	0
Broadcast	426	0

TX Packets	Total	Total/sec
Bytes	25930758	39344
Packets	30663	49

Figure 11-5 RX Packets Analysis Table window

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.

Click the **Apply** button to accept the changes made.

Click the **Clear** button to clear all statistics counters on this window.

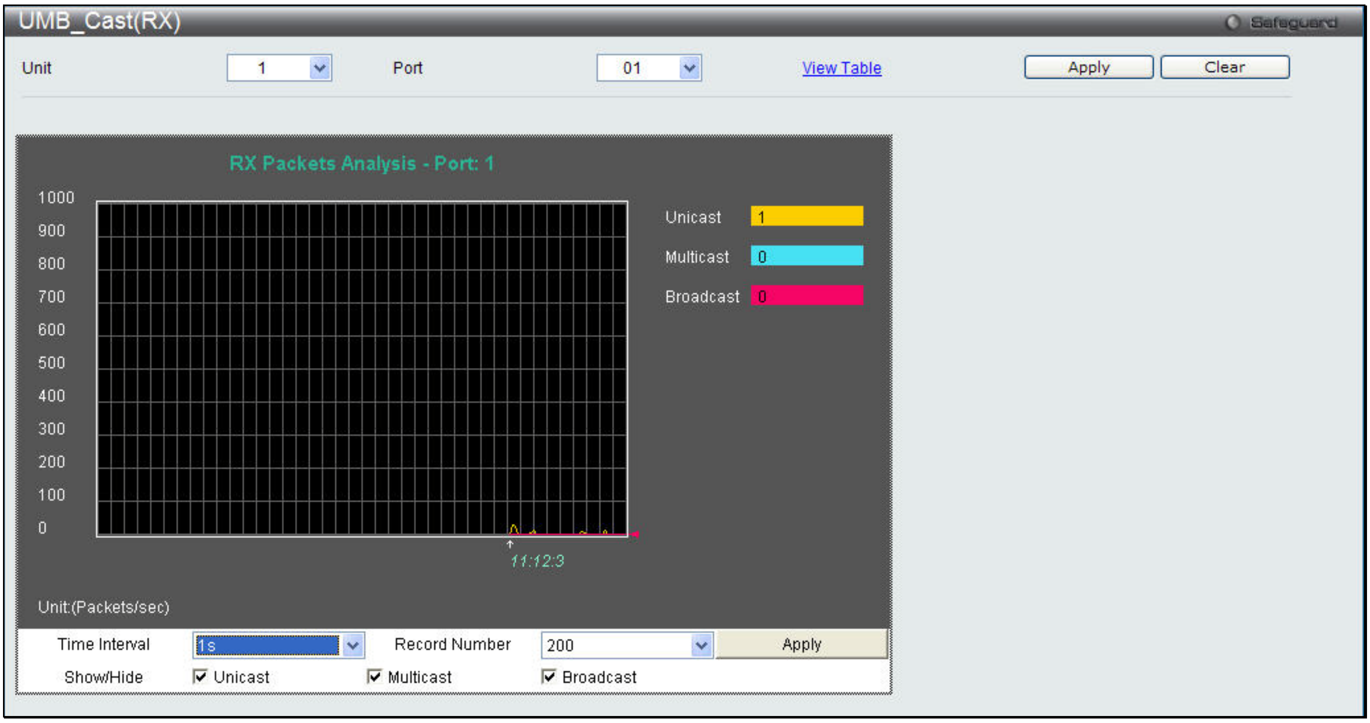
Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

UMB_Cast (RX)

To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Port Statistics > Packets > UMB_Cast (RX)** as shown below:


UMB_Cast(RX)
Safeguard
View Table
Apply
Clear
RX Packets Analysis - Port: 1
1000
900
800
700
600
500
400
300
200
100
0
11:12:3
Unit:(Packets/sec)
Apply

Unit: 1

Port: 01

Unicast: 1

Multicast: 0

Broadcast: 0

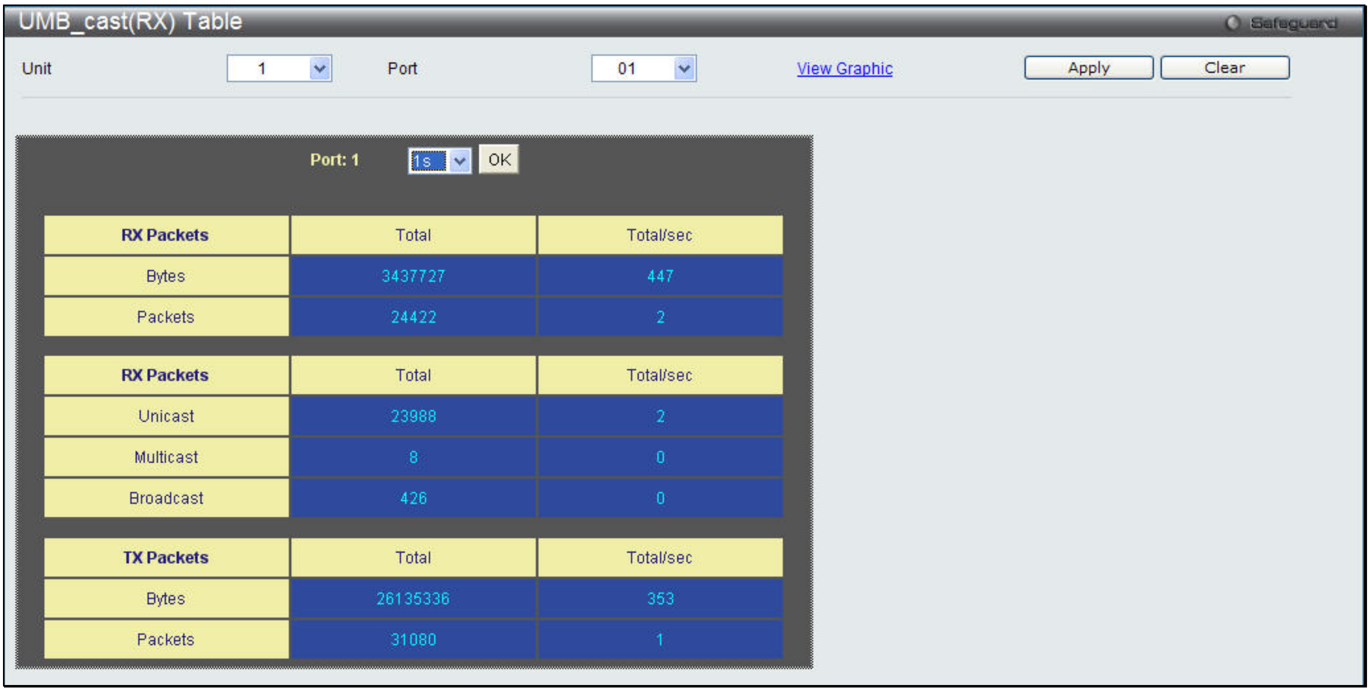
Time Interval: 1s

Record Number: 200

Show/Hide: ☑ Unicast ☑ Multicast ☑ Broadcast

Figure 11-6 UMB_cast (RX) window (for Unicast, Multicast, and Broadcast Packets)

Click the View Table link to display the information in a table rather than a line graph.


UMB_cast(RX) Table
Safeguard
View Graphic
Apply
Clear
OK

Unit: 1

Port: 01

Port: 1 — 1s

RX Packets	Total	Total/sec
Bytes	3437727	447
Packets	24422	2

RX Packets	Total	Total/sec
Unicast	23988	2
Multicast	8	0
Broadcast	426	0

TX Packets	Total	Total/sec
Bytes	26135336	353
Packets	31080	1

Figure 11-7 RX Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

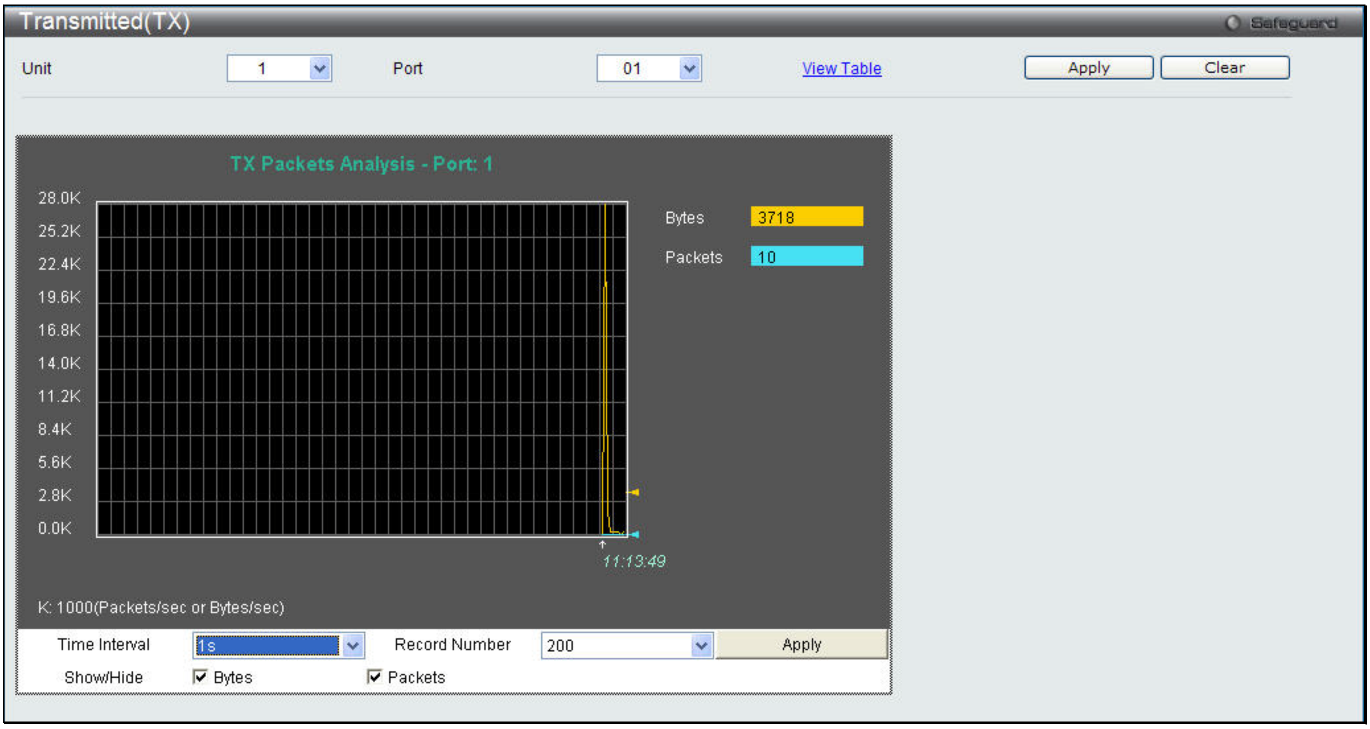
Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Port Statistics > Packets > Transmitted (TX)** as shown below:


Transmitted(TX)
Safeguard
View Table
Apply
Clear
TX Packets Analysis - Port: 1
28.0K
25.2K
22.4K
19.6K
16.8K
14.0K
11.2K
8.4K
5.6K
2.8K
0.0K
11:13:49
K: 1000(Packets/sec or Bytes/sec)
Apply

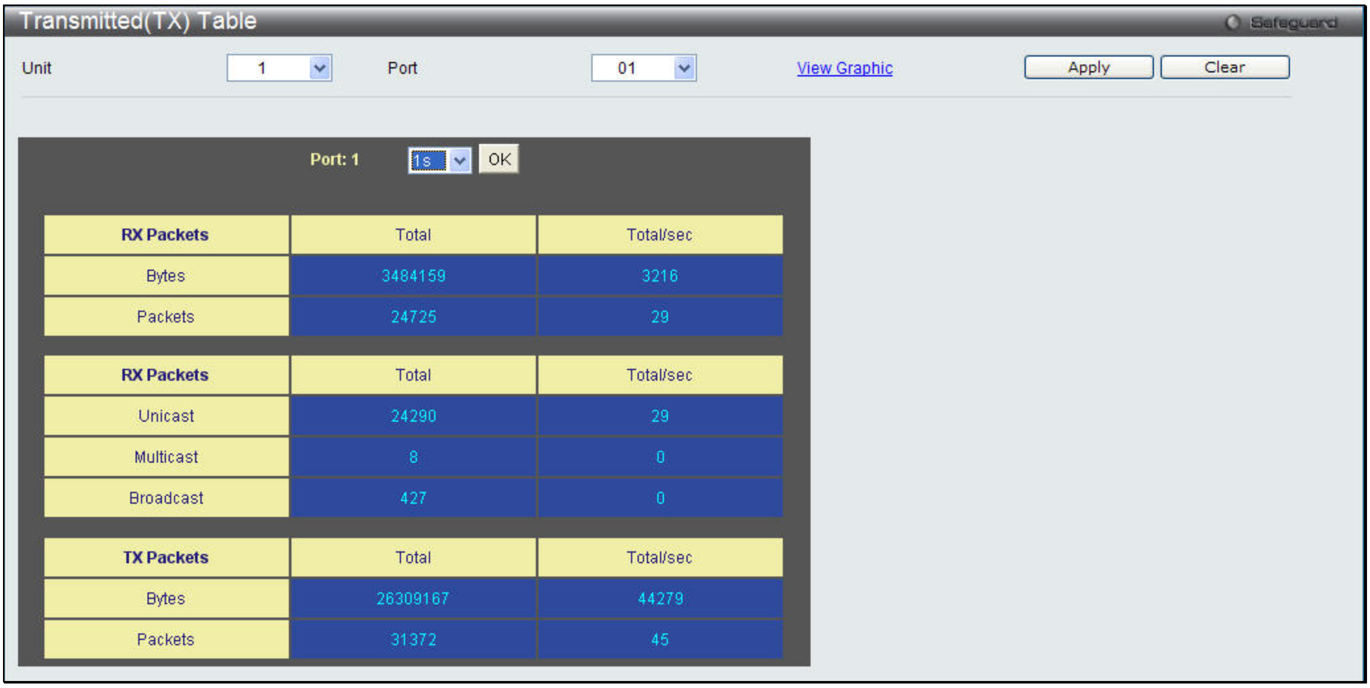
Unit: 1
Port: 01

Bytes: 3718
Packets: 10

Time Interval: 1s
Record Number: 200
Show/Hide: ☑ Bytes ☑ Packets

Figure 11-8 Transmitted (TX) window (for Bytes and Packets)

Click the View Table link to display the information in a table rather than a line graph.



Unit 1

Port 01

Port: 1 1s

RX Packets	Total	Total/sec
Bytes	3484159	3216
Packets	24725	29

RX Packets	Total	Total/sec
Unicast	24290	29
Multicast	8	0
Broadcast	427	0

TX Packets	Total	Total/sec
Bytes	26309167	44279
Packets	31372	45

Figure 11-9 TX Packets Analysis window (table for Bytes and Packets)

The fields that can be configured or displayed are described below:

Parameter	Description
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

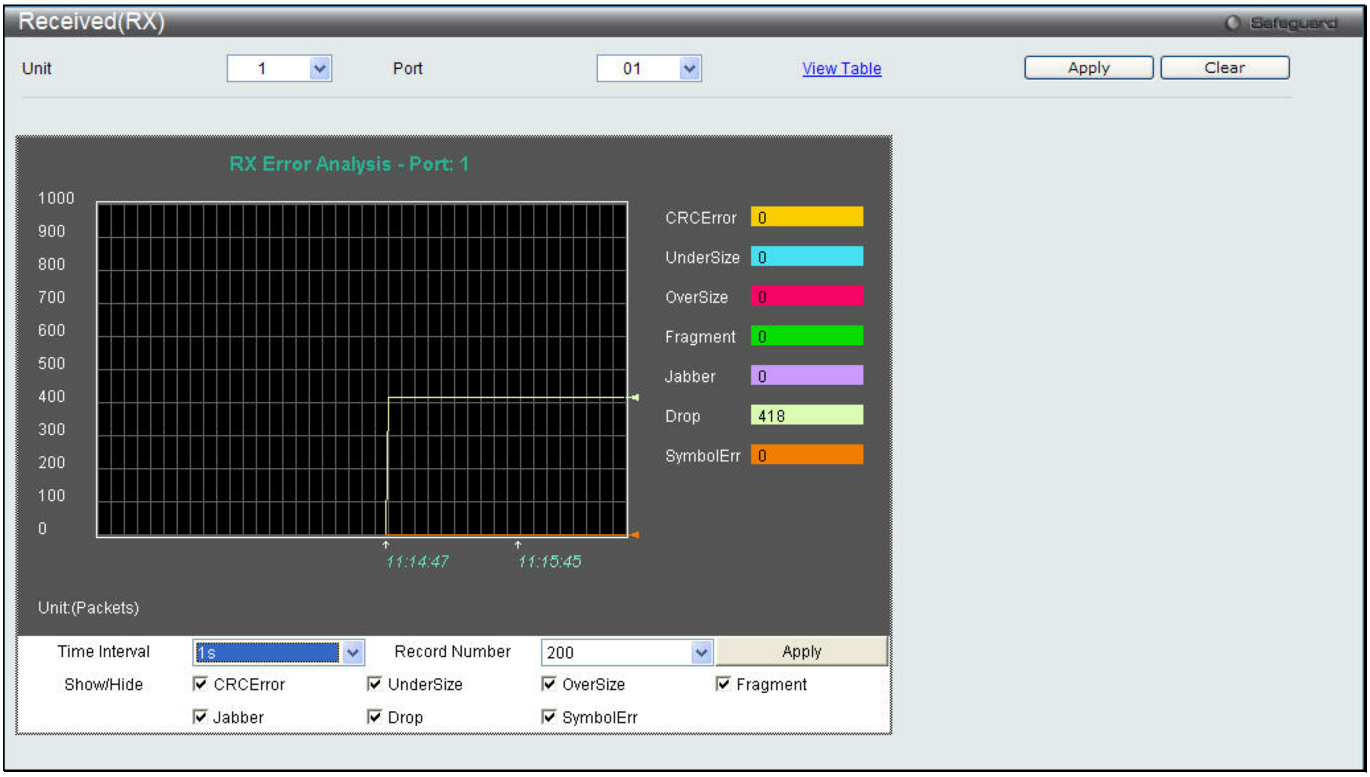
Errors

The Web manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Port Statistics > Errors > Received (RX)** as shown below:


Received(RX)
Safeguard
View Table
Apply
Clear
RX Error Analysis - Port: 1
1000
900
800
700
600
500
400
300
200
100
0
11:14:47
11:15:45
Unit:(Packets)
Apply

Unit: 1

Port: 01

CRCError: 0

UnderSize: 0

OverSize: 0

Fragment: 0

Jabber: 0

Drop: 418

SymbolErr: 0

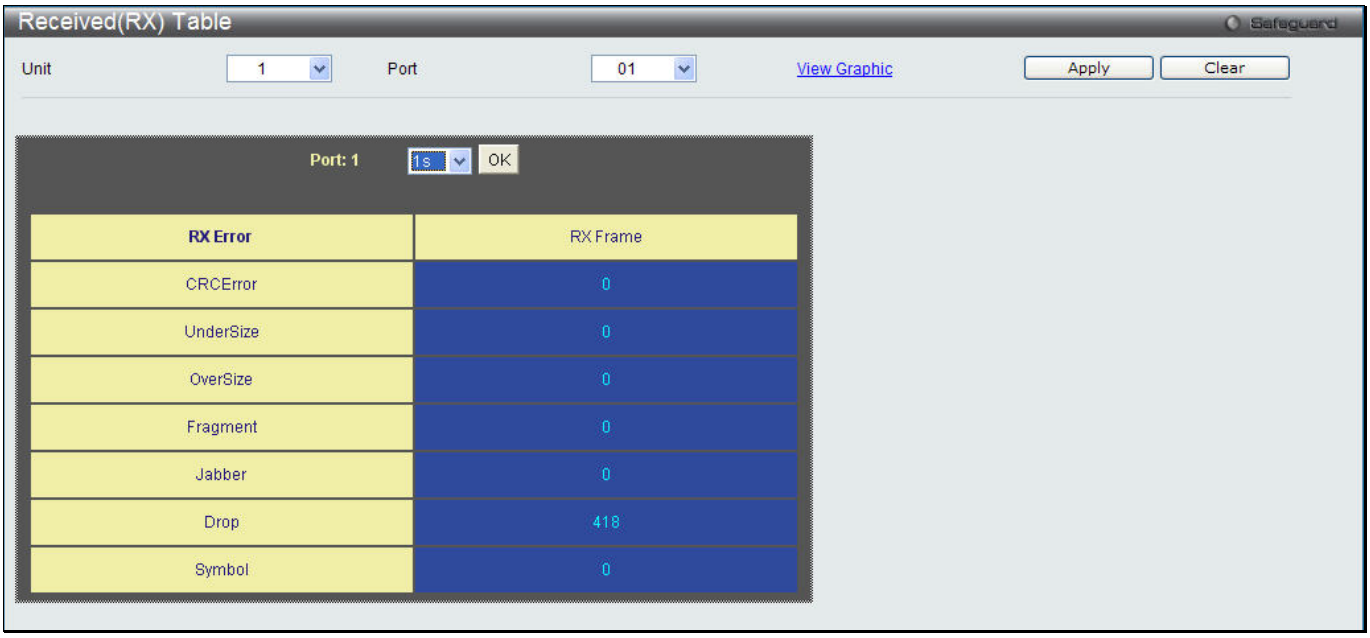
Time Interval: 1s

Record Number: 200

Show/Hide: ☑ CRCError ☑ UnderSize ☑ OverSize ☑ Fragment ☑ Jabber ☑ Drop ☑ SymbolErr

Figure 11-10 Received (RX) window (for errors)

Click the View Table link to display the information in a table rather than a line graph.


Received(RX) Table
Safeguard
View Graphic
Apply
Clear
OK

Unit: 1

Port: 01

Port: 1 1s

RX Error	RX Frame
CRCError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop	418
Symbol	0

Figure 11-11 RX Error Analysis window (table)

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value

	is *200*.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Symbol	Counts the number of packets received that have errors received in the symbol on the physical labor.
Show/Hide	Check whether or not to display CRCError, UnderSize, OverSize, Fragment, Jabber, Drop, and SymbolErr errors.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

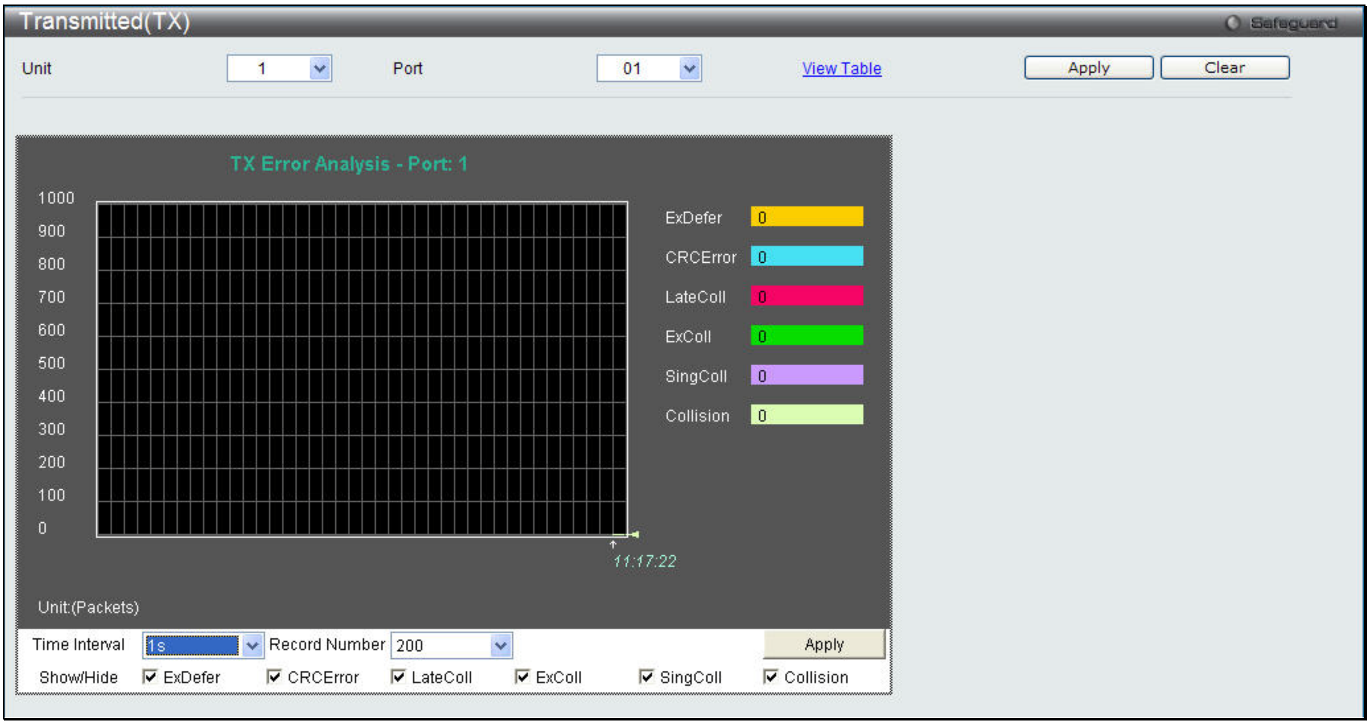
Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Port Statistics > Errors > Transmitted (TX)** as shown below:



Unit 1

Port 01

ExDefer 0

CRCError 0

LateColl 0

ExColl 0

SingColl 0

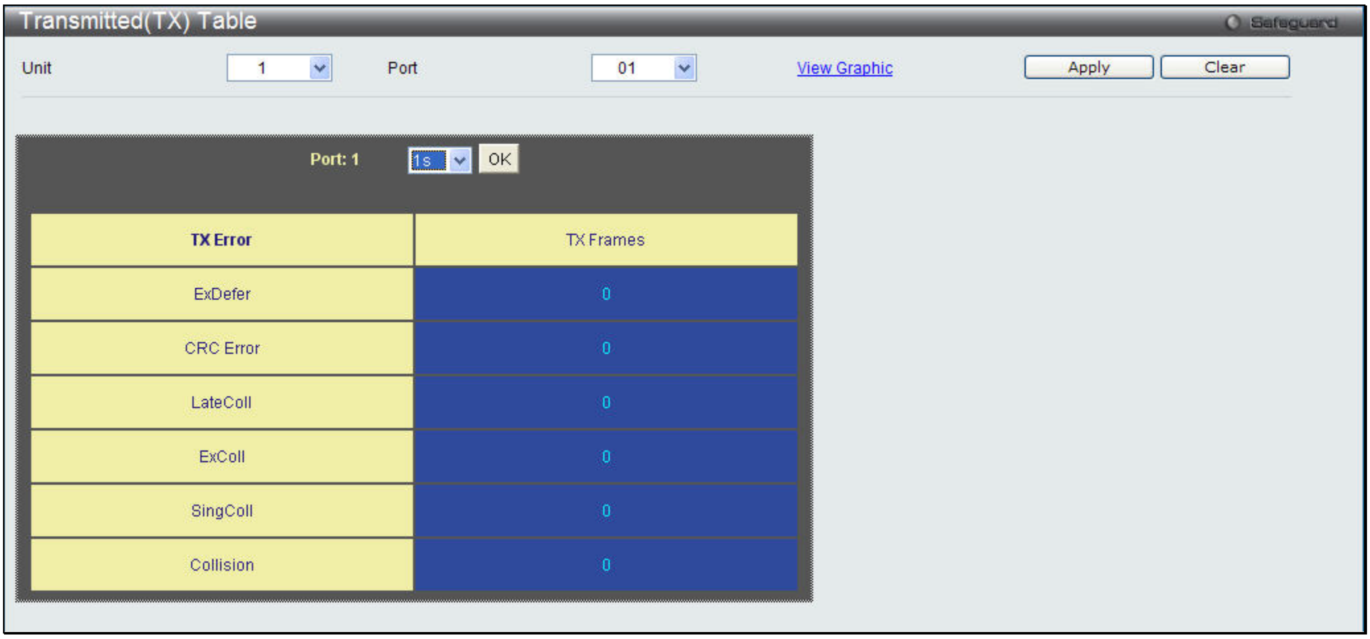
Collision 0

Time Interval 1s

Record Number 200

Figure 11-12 Transmitted (TX) window (for errors)

Click the View Table link to display the information in a table rather than a line graph.



TX Error	TX Frames
ExDefer	0
CRC Error	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

Figure 11-13 TX Error Analysis window (table)

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Collision	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, CRCError, LateColl, ExColl, SingColl, and Collision errors.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

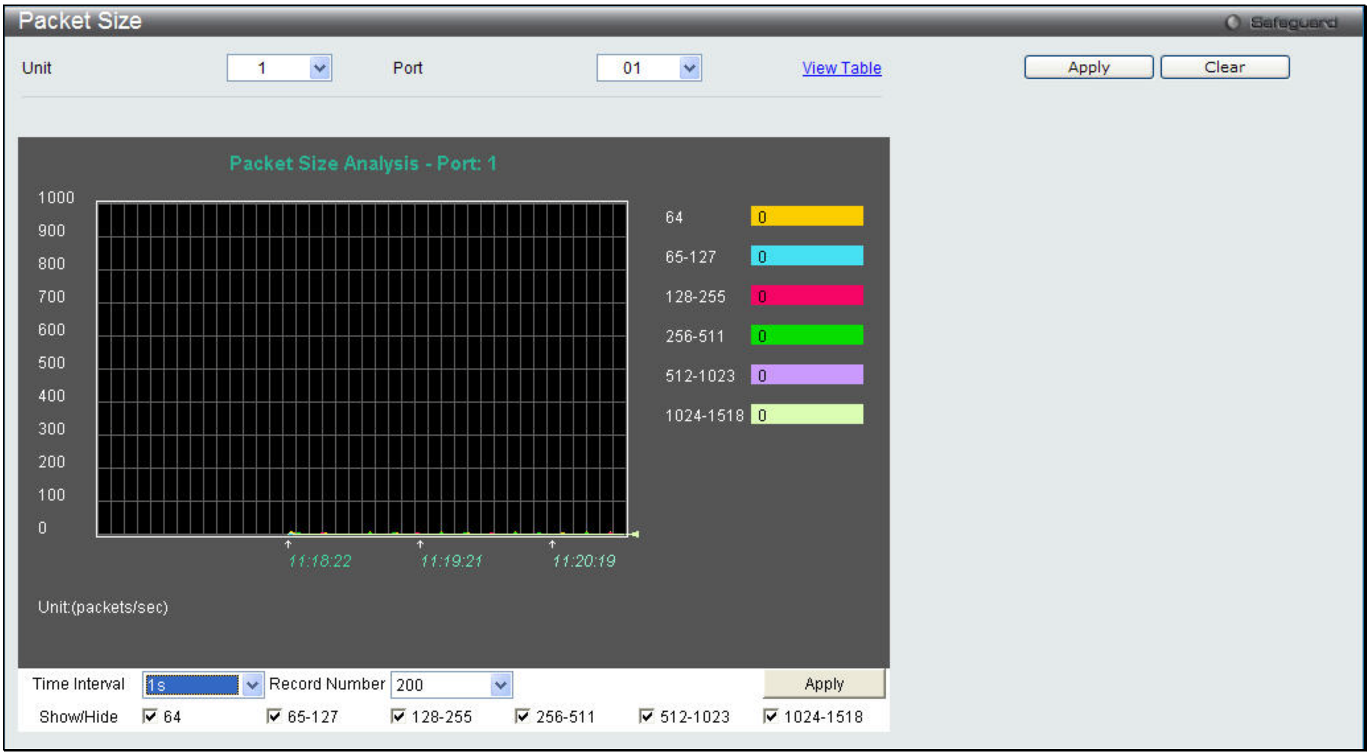
Click the View Table link to display the information in a table rather than a line graph.

Click the View Graphic link to display the information in a line graph rather than a table.

Packet Size

Users can display packets received by the Switch, arranged in six groups and classed by size, as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the Port drop-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Statistics > Packet Size** as shown below:


Packet Size
Safeguard
View Table
Apply
Clear
Packet Size Analysis - Port: 1
1000
900
800
700
600
500
400
300
200
100
0
11:18:22
11:19:21
11:20:19
Unit:(packets/sec)
Apply

Unit: 1

Port: 01

64	0
65-127	0
128-255	0
256-511	0
512-1023	0
1024-1518	0

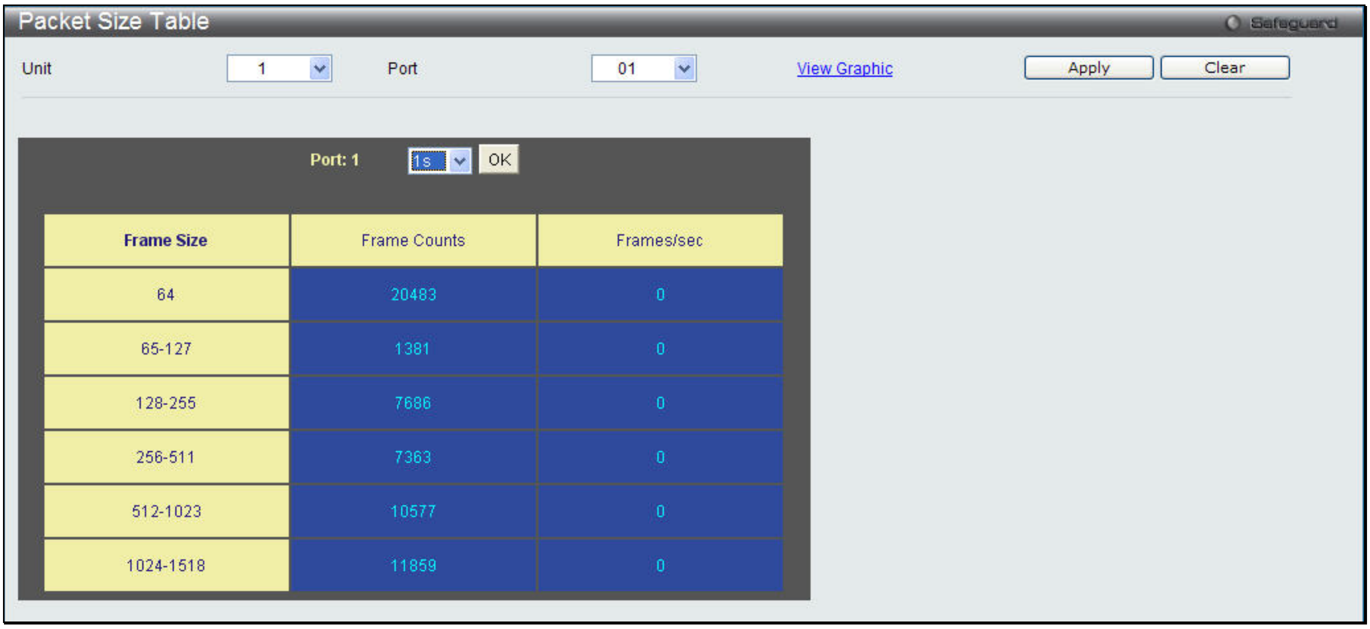
Time Interval: 1s

Record Number: 200

Show/Hide: ☑ 64 ☑ 65-127 ☑ 128-255 ☑ 256-511 ☑ 512-1023 ☑ 1024-1518

Figure 11-14 Packet Size window

Click the View Table link to display the information in a table rather than a line graph.


Packet Size Table
Safeguard
View Graphic
Apply
Clear
OK

Unit: 1

Port: 01

Port: 1 — 1s

Frame Size	Frame Counts	Frames/sec
64	20483	0
65-127	1381	0
128-255	7686	0
256-511	7363	0
512-1023	10577	0
1024-1518	11859	0

Figure 11-15 RX Size Analysis window (table)

The fields that can be configured or displayed are described below:

Parameter	Description
Unit	Select the unit you want to configure.
Port	Use the drop-down menu to choose the port that will display statistics.
Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.

Click the **Apply** button to accept the changes made for each individual section.

Click the **Clear** button to clear all statistics counters on this window.

Click the View Table link to display the information in a table rather than a line graph.

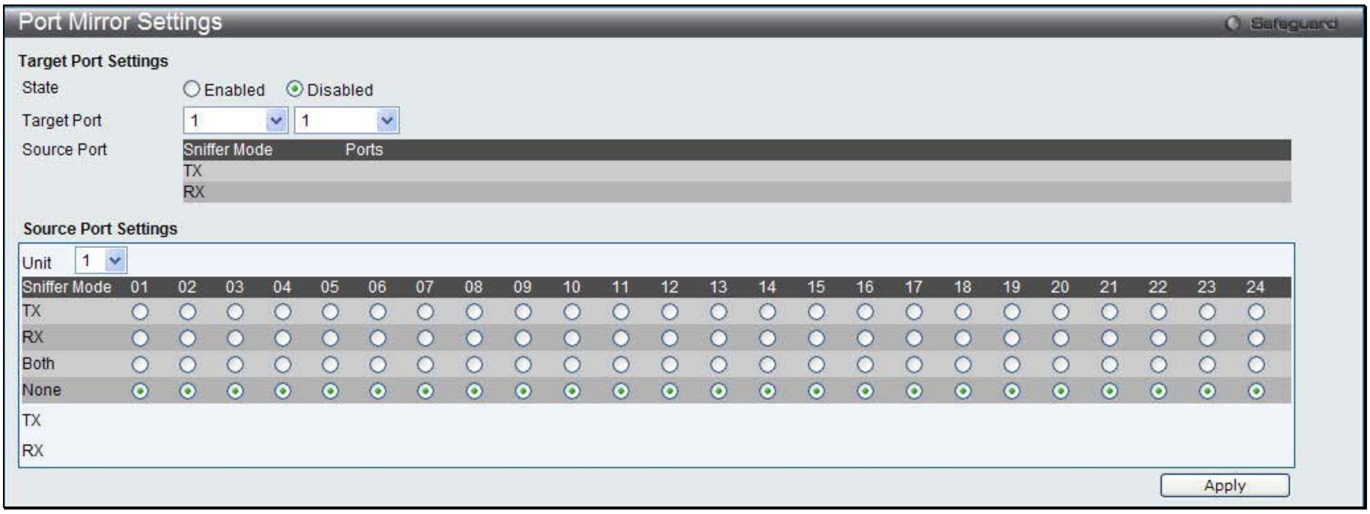
Click the View Graphic link to display the information in a line graph rather than a table.

Mirror

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Port Mirror Settings

To view this window, click **Monitoring > Mirror > Port Mirror Settings** as shown below:



Target Port Settings

State ○ Enabled ● Disabled

Target Port 1 1

Source Port

Sniffer Mode	Ports
TX	
RX	

Source Port Settings

Unit 1

Sniffer Mode	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
TX	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
RX	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Both	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

TX

RX

Figure 11-16 Port Mirror Settings window

The fields that can be configured are described below:

Parameter	Description
State	Click the radio buttons to enable or disable the Port Mirroring feature.
Target Port	Use the drop-down menu to select the Target Port used for Port Mirroring.
Unit	Select the unit you want to configure.
TX (Egress)	Click the radio buttons to select whether the port should include outgoing traffic.
RX (Ingress)	Click the radio buttons to select whether the port should include incoming traffic.
Both	Click the radio buttons to select whether the port should include both incoming and outgoing traffic.
None	Click the radio buttons to select whether the port should not include any traffic.

Click the **Apply** button to accept the changes made.

NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

RSPAN Settings

This page controls the RSPAN function. The purpose of the RSPAN function is to mirror packets to a remote switch. A packet travels from the switch where the monitored packet is received, passing through the intermediate switch, and then to the switch where the sniffer is attached. The first switch is also named the source switch.

To make the RSPAN function work, the RSPAN VLAN source setting must be configured on the source switch. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured.

NOTE: RSPAN VLAN mirroring will only work when RSPAN is enabled (when one RSPAN VLAN has been configured with a source port). The RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

To view this window, click **Monitoring > Mirror > RSPAN Settings** as shown below:

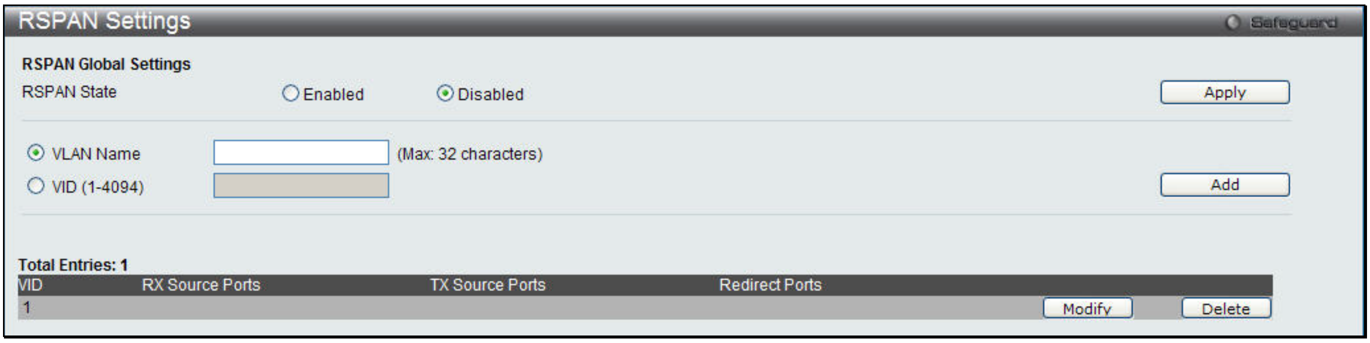

RSPAN Settings
Safeguard
RSPAN Global Settings
RSPAN State
○ Enabled
● Disabled
Apply
● VLAN Name
(Max: 32 characters)
○ VID (1-4094)
Add
Total Entries: 1
VID
RX Source Ports
TX Source Ports
Redirect Ports
1
Modify
Delete

Figure 11-17 RSPAN Settings window

The fields that can be configured are described below:

Parameter	Description
RSPAN State	Click the radio buttons to enable or disable the RSPAN feature.
VLAN Name	Create the RSPAN VLAN by VLAN name.
VID (1-4094)	Create the RSPAN VLAN by VLAN ID.

Click the **Apply** button to accept the changes made.

Click the **Add** button to add a new entry based on the information entered.

Click the **Modify** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

After clicking the **Modify** button, the following page will appear:

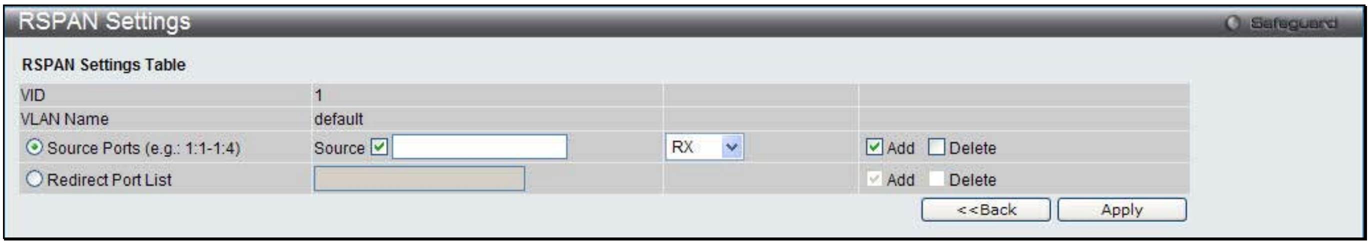

RSPAN Settings
Safeguard
RSPAN Settings Table
VID
1
VLAN Name
default
● Source Ports (e.g.: 1:1-1:4)
Source ☑
RX
☑ Add
☐ Delete
○ Redirect Port List
☑ Add
☐ Delete
<<Back
Apply

Figure 11-18 RSPAN Settings – Modify window

The fields that can be configured are described below:

Parameter	Description
VID	Displays the RSPAN VLAN by VLAN ID.
VLAN Name	Displays the RSPAN VLAN by VLAN name.
Source Ports	If the ports are not specified by option, the source of RSPAN will come from the source specified by the mirror command or the flow-based source specified by an ACL. If no parameter is specified for source, it deletes the configured source parameters. Select **RX, TX** or **Both** to specify in which direction the packets will be monitored. Tick **Add** or **Delete** to add or delete source ports.
Redirect Port List	Specify the output port list for the RSPAN VLAN packets. If the redirect port is a Link Aggregation port, the Link Aggregation behavior will apply to the RSPAN packets. Tick **Add** or **Delete** to add or delete redirect ports.

Click the **Apply** button to accept the changes made.

Click the **<<Back** button to discard the changes made and return to the previous page.

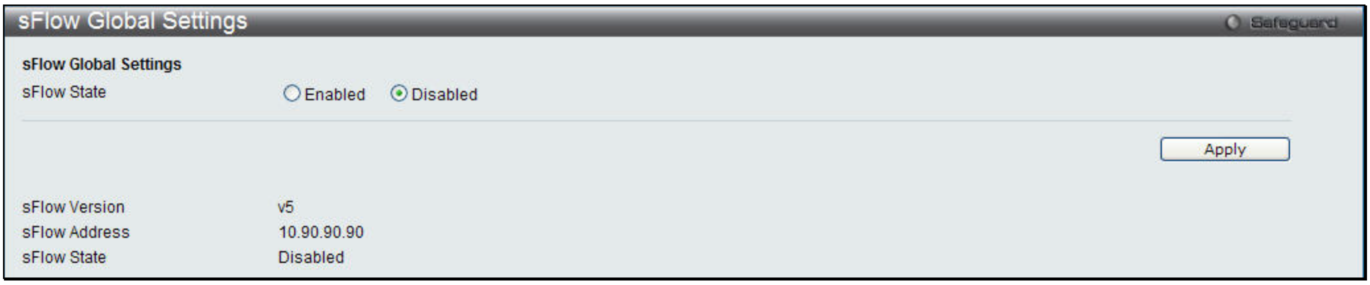
sFlow (EI Mode Only)

sFlow (RFC3176) is a technology for monitoring traffic in data networks containing switches and routers. The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The architecture and sampling techniques used in the sFlow monitoring system were designed for providing continuous site-wide (and enterprise-wide) traffic monitoring of high speed switched and routed networks.

sFlow Global Settings

This window is used to enable or disable the sFlow feature.

To view this window, click **Monitoring > sFlow > sFlow Global Settings** as shown below:



sFlow Global Settings

sFlow State ○ Enabled ● Disabled

sFlow Version	v5
sFlow Address	10.90.90.90
sFlow State	Disabled

Figure 11-19 sFlow Global Settings window

The fields that can be configured are described below:

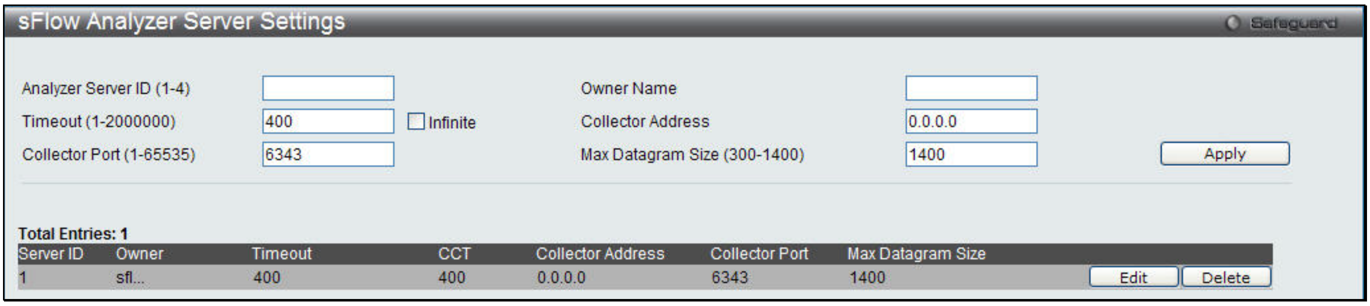
Parameter	Description
sFlow State	Here the user can enable or disable the sFlow feature.

Click the **Apply** button to accept the changes made.

sFlow Analyzer Server Settings

The Switch can support 4 different Analyzer Servers at the same time and each sampler or poller can select a collector to send the samples. We can send different samples from different samplers or pollers to different collectors.

To view this window, click **Monitoring > sFlow > sFlow Analyzer Server Settings** as shown below:



Analyzer Server ID (1-4)			Owner Name	
Timeout (1-2000000)	400	☐ Infinite	Collector Address	0.0.0.0
Collector Port (1-65535)	6343		Max Datagram Size (300-1400)	1400

Total Entries: 1

Server ID	Owner	Timeout	CCT	Collector Address	Collector Port	Max Datagram Size		
1	sfl...	400	400	0.0.0.0	6343	1400	Edit	Delete

Figure 11-20 sFlow Analyzer Server Settings window

The fields that can be configured are described below:

Parameter	Description
Analyzer Server ID (1-4)	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Owner Name	The entity making use of this sFlow analyzer server. When owner is set or modified, the timeout value will become 400 automatically.

Timeout (1-2000000)	The length of time before the server times out. When the analyzer server times out, all of the flow samplers and counter pollers associated with this analyzer server will be deleted. If not specified, its default value is 400.
Collector Address	The IP address of the analyzer server. If not specified or set a 0 address, the entry will be inactive.
Collector Port (1-65535)	The destination UDP port for sending the sFlow datagrams. If not specified, the default value is *6343.*
Max Datagram Size (300-1400)	The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.

Click the **Apply** button to accept the changes made.

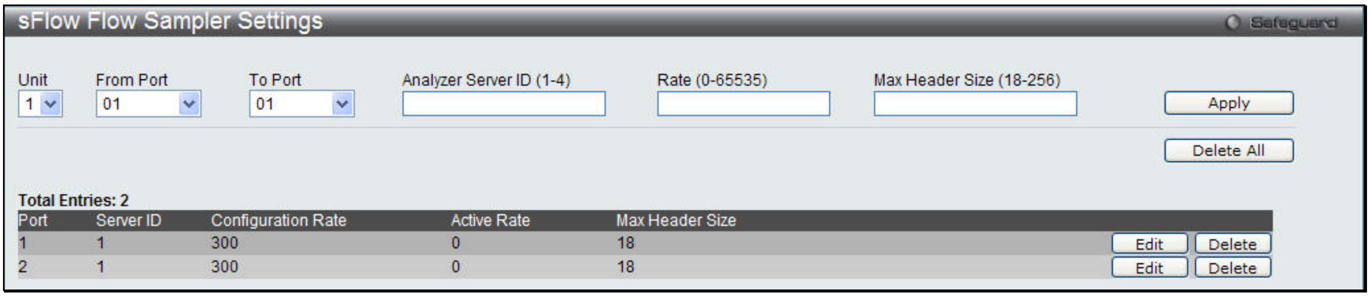
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

sFlow Flow Sampler Settings

On this page the user can configure the sFlow flow sampler parameters. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.

NOTE: If the user wants the change the analyze server ID, he needs to delete the flow sampler and creates a new one.



Unit: 1
From Port: 01
To Port: 01

Total Entries: 2

Port	Server ID	Configuration Rate	Active Rate	Max Header Size		
1	1	300	0	18	Edit	Delete
2	1	300	0	18	Edit	Delete

Figure 11-21 sFlow Flow Sampler Settings window

The fields that can be configured are described below:

Parameter	Description
Unit	Select a unit to configure.
From Port / To Port	Use the drop-down menus to specify the list of ports to be configured.
Analyzer Server ID (1-4)	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Rate (0-65535)	The sampling rate for packet Rx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. The sampling rate for packet Tx sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from every 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0.
MAX Header Size (18-256)	The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.

Click the **Apply** button to accept the changes made.

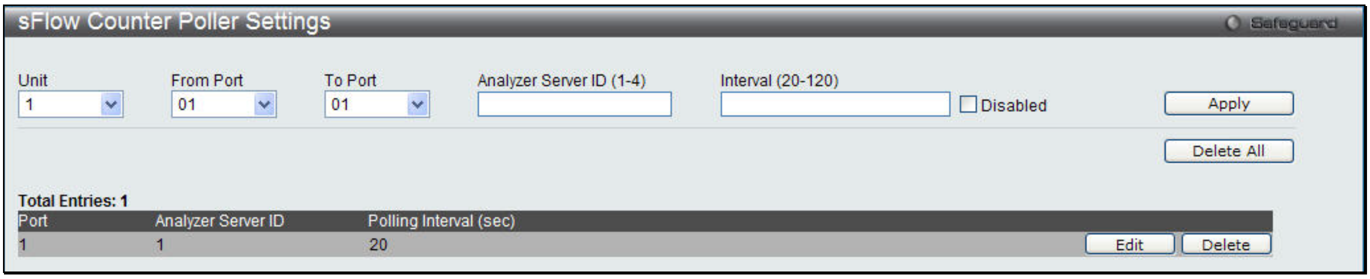
Click the **Delete All** button to remove all the entries listed.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

sFlow Counter Poller Settings

On this page the user can configure the sFlow counter poller parameters. If the user wants to change the analyzer server ID, he needs to delete the counter poller and create a new one.



Unit: 1
From Port: 01
To Port: 01
Analyzer Server ID (1-4):
Interval (20-120): ☐ Disabled

Total Entries: 1

Port	Analyzer Server ID	Polling Interval (sec)
1	1	20

Figure 11-22 sFlow Counter Poller Settings

The fields that can be configured are described below:

Parameter	Description
Unit	Select a unit to configure.
From Port / To Port	Use the drop-down menus to specify the list of ports to be configured.
Analyzer Server ID (1-4)	The analyzer server ID specifies the ID of a server analyzer where the packet will be forwarded.
Interval (20-120)	The maximum number of seconds between successive samples of the counters. Tick the **Disabled** check box to disable the polling interval.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries listed.

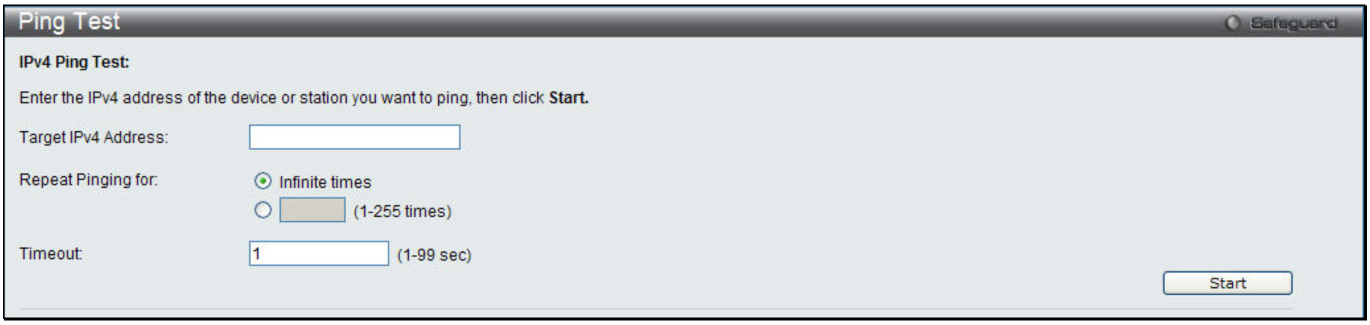
Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

To view this window, click **Monitoring > Ping Test** as shown below:



IPv4 Ping Test:

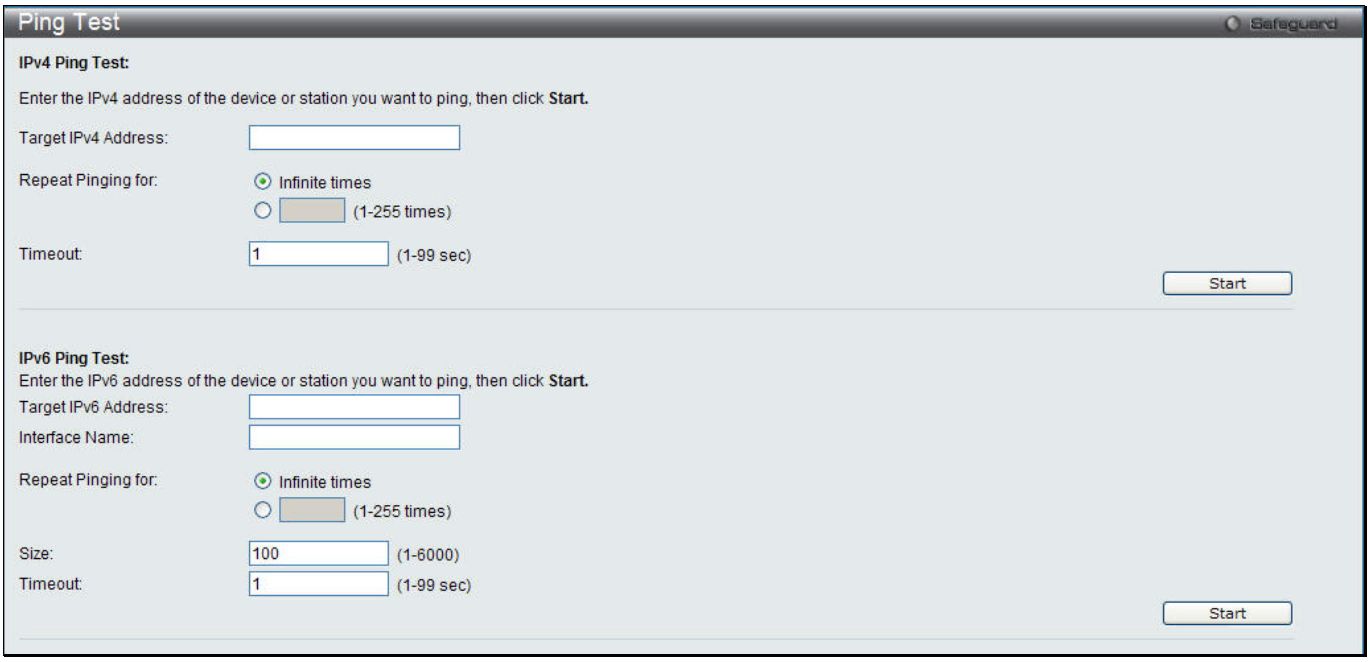
Enter the IPv4 address of the device or station you want to ping, then click **Start.**

Target IPv4 Address:

Repeat Pinging for: ● Infinite times
○ (1-255 times)

Timeout: 1 (1-99 sec)

Figure 11-23 Ping Test window (SI Mode Only)



IPv4 Ping Test:

Enter the IPv4 address of the device or station you want to ping, then click **Start.**

Target IPv4 Address:

Repeat Pinging for: ● Infinite times ○ (1-255 times)

Timeout: 1 (1-99 sec)

IPv6 Ping Test:

Enter the IPv6 address of the device or station you want to ping, then click **Start.**

Target IPv6 Address:

Interface Name:

Repeat Pinging for: ● Infinite times ○ (1-255 times)

Size: 100 (1-6000)

Timeout: 1 (1-99 sec)

Figure 11-24 Ping Test window (EI Mode Only)

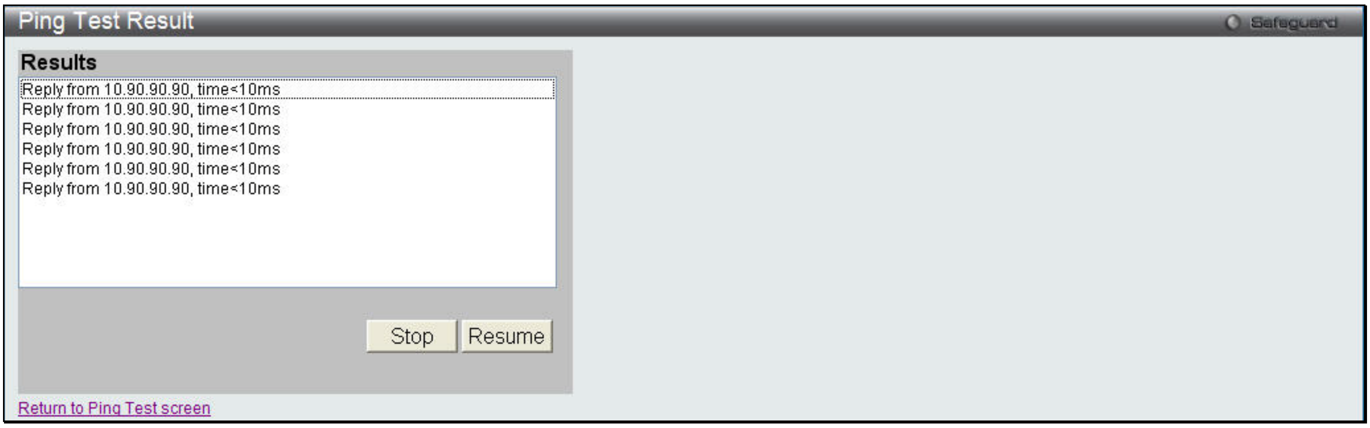
The user may click the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between *1* and *255*.

The fields that can be configured are described below:

Parameter	Description
Target IPv4 Address	Enter an IP address to be pinged.
Target IPv6 Address (EI Mode Only)	Enter an IPv6 address to be pinged.
Repeat Pinging for	Enter the number of times desired to attempt to Ping either the IPv4 address or the IPv6 address configured in this window. Users may enter a number of times between *1* and *255*.
Size (EI Mode Only)	For IPv6 only, enter a value between *1* and *6000*. The default is *100*.
Timeout	Select a timeout period between *1* and *99* seconds for this Ping message to reach its destination. If the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

Click the **Start** button to initiate the Ping Test.

After clicking the **Start** button, the following page will appear:



Results

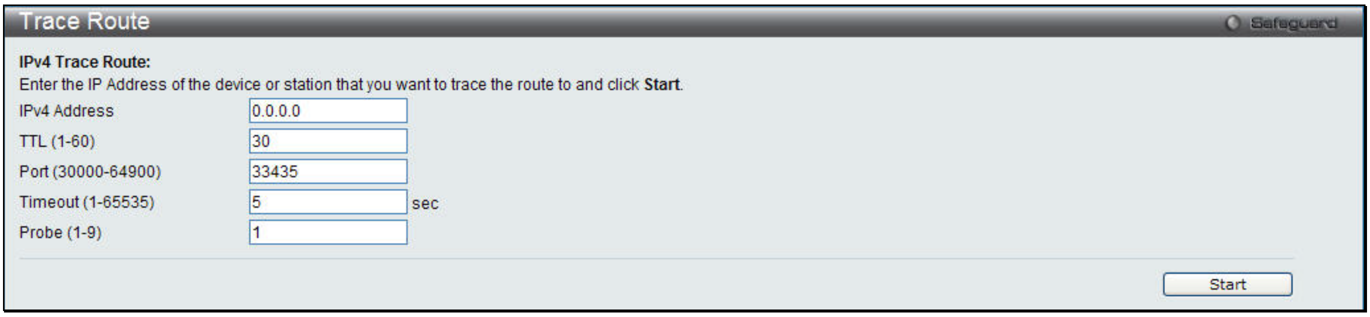
Reply from 10.90.90.90, time<10ms
Reply from 10.90.90.90, time<10ms
Reply from 10.90.90.90, time<10ms
Reply from 10.90.90.90, time<10ms
Reply from 10.90.90.90, time<10ms
Reply from 10.90.90.90, time<10ms

Figure 11-25 Ping Test Result window

Click the **Stop** button to halt the Ping Test.
Click the **Resume** button to resume the Ping Test.

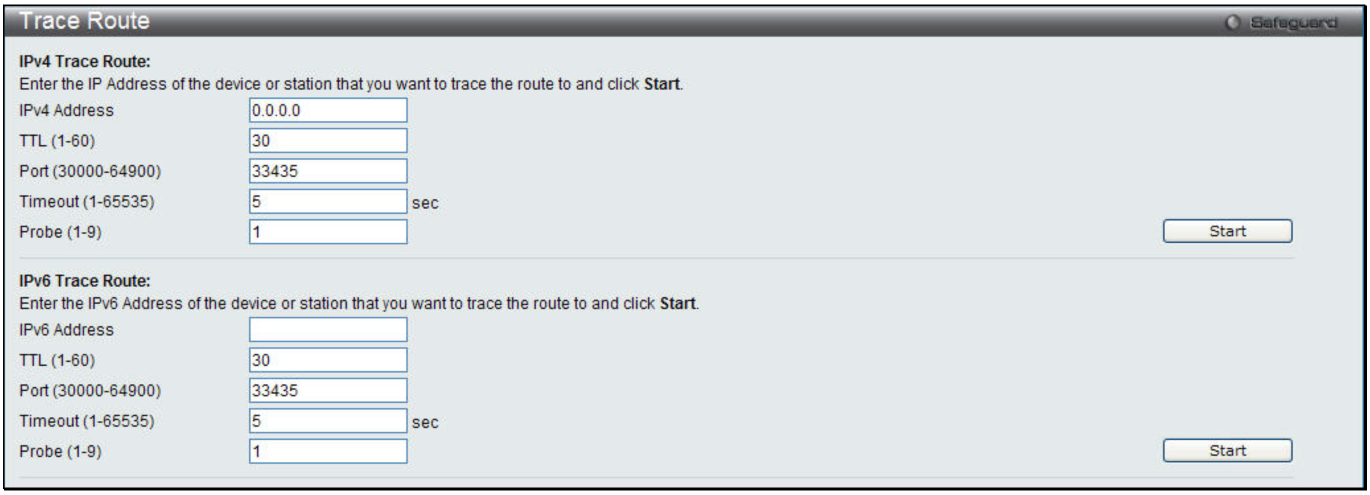
Trace Route

The trace route page allows the user to trace a route between the switch and a given host on the network.
To view this window, click **Monitoring > Trace Route** as shown below:



IPv4 Trace Route:
Enter the IP Address of the device or station that you want to trace the route to and click **Start**.
IPv4 Address: 0.0.0.0
TTL (1-60): 30
Port (30000-64900): 33435
Timeout (1-65535): 5 sec
Probe (1-9): 1

Figure 11-26 Trace Route window (SI Mode Only)



IPv4 Trace Route:
Enter the IP Address of the device or station that you want to trace the route to and click **Start**.
IPv4 Address: 0.0.0.0
TTL (1-60): 30
Port (30000-64900): 33435
Timeout (1-65535): 5 sec
Probe (1-9): 1

IPv6 Trace Route:
Enter the IPv6 Address of the device or station that you want to trace the route to and click **Start**.
IPv6 Address:
TTL (1-60): 30
Port (30000-64900): 33435
Timeout (1-65535): 5 sec
Probe (1-9): 1

Figure 11-27 Trace Route window (EI Mode Only)

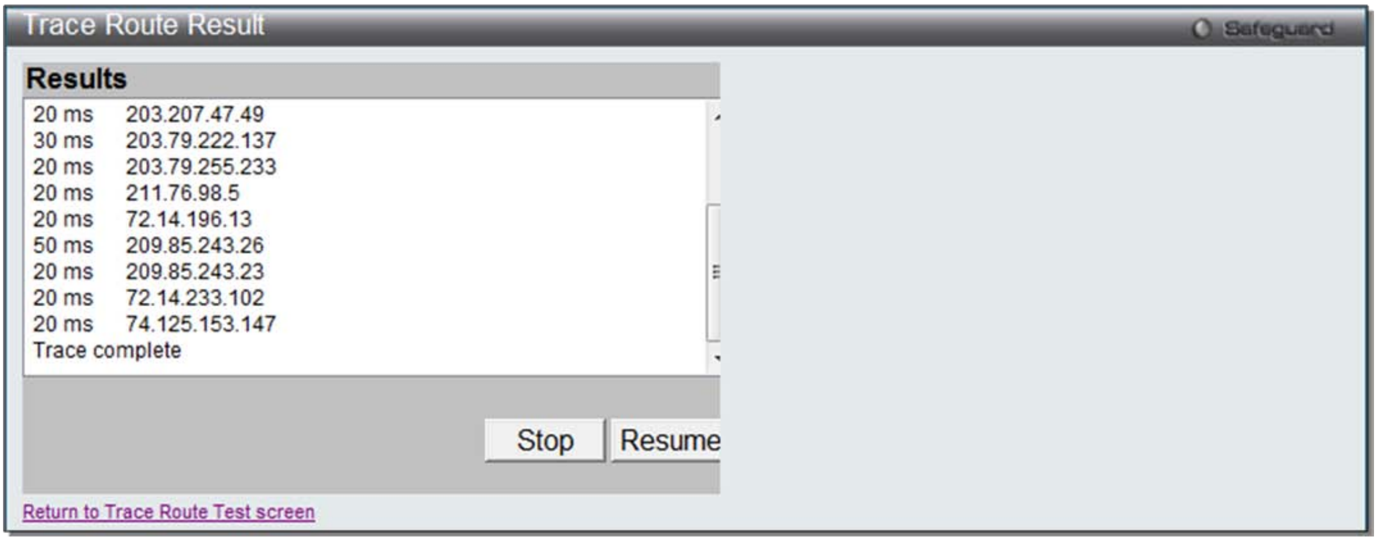
The fields that can be configured are described below:

Parameter	Description
IPv4 Address	IP address of the destination station.
IPv6 Address	IPv6 address of the destination station.

TTL (1-60)	The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.
Port (30000-64900)	The port number. The value range is from 30000 to 64900.
Timeout (1-65535)	Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
Probe (1-9)	The number of probing. The range is from 1 to 9. If unspecified, the default value is 1.

Click the **Start** button to initiate the Trace Route.

After clicking the **Start** button, the following page will appear:



```
20 ms    203.207.47.49
30 ms    203.79.222.137
20 ms    203.79.255.233
20 ms    211.76.98.5
20 ms    72.14.196.13
50 ms    209.85.243.26
20 ms    209.85.243.23
20 ms    72.14.233.102
20 ms    74.125.153.147
Trace complete
```

Figure 11-28 Trace Route Result window

Click the **Stop** button to halt the Trace Route.

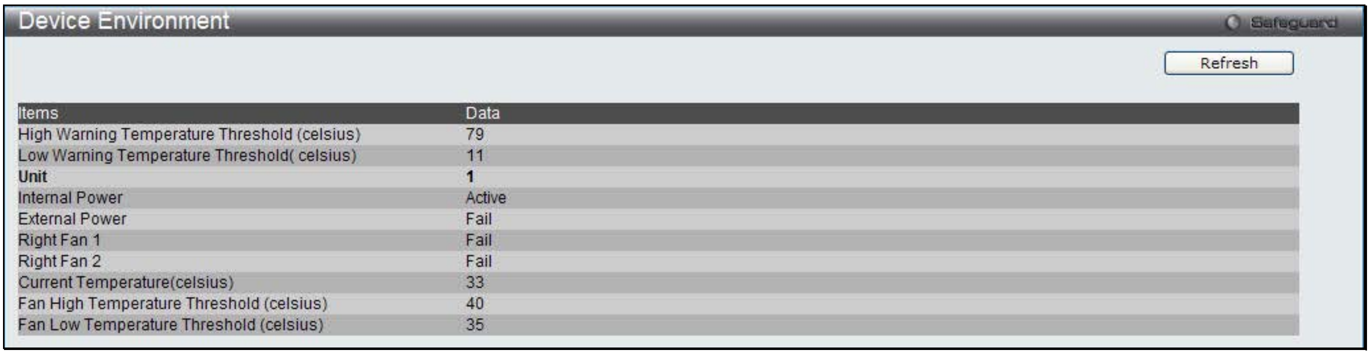
Click the **Resume** button to resume the Trace Route.

Peripheral

Device Environment

The device environment feature displays the Switch internal temperature status.

To view this window, click **Monitoring > Peripheral > Device Environment** as shown below:



Items	Data
High Warning Temperature Threshold (celsius)	79
Low Warning Temperature Threshold(celsius)	11
Unit	**1**
Internal Power	Active
External Power	Fail
Right Fan 1	Fail
Right Fan 2	Fail
Current Temperature(celsius)	33
Fan High Temperature Threshold (celsius)	40
Fan Low Temperature Threshold (celsius)	35

Figure 11-29 Device Environment window

Click the **Refresh** button to refresh the display table so that new entries will appear.

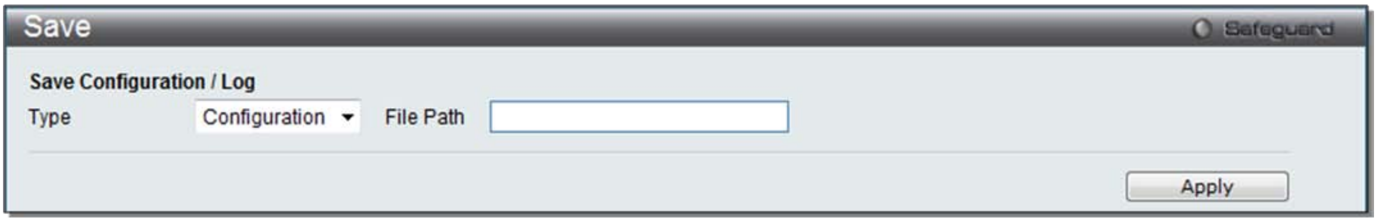
Chapter 12 Save and Tools

Save Configuration / Log
Stacking Information
Download firmware
Upload Firmware
Download Configuration
Upload Configuration
Upload Log File
Reset
Reboot System

Save Configuration / Log

To view this window, click **Save > Save Configuration / Log**, as shown below.

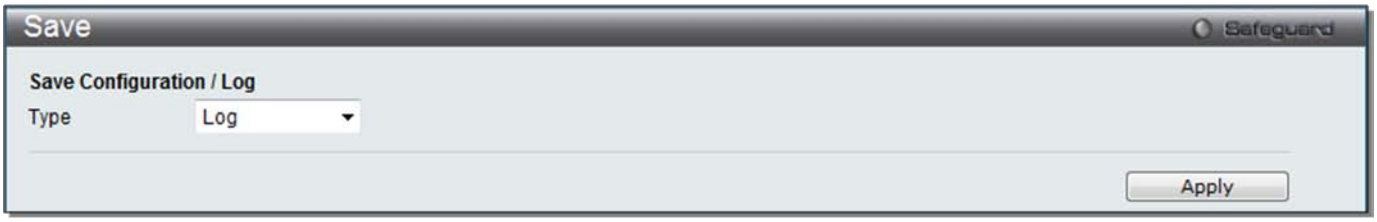
Save Configuration allows the user to backup the configuration of the switch to a folder on the computer. Select **Configuration** from the **Type** drop-down menu and enter the **File Path** in the space provided and click **Apply**.


Save
Safeguard
Save Configuration / Log
File Path
Apply

Type Configuration

Figure 12-1 Save – Configuration window

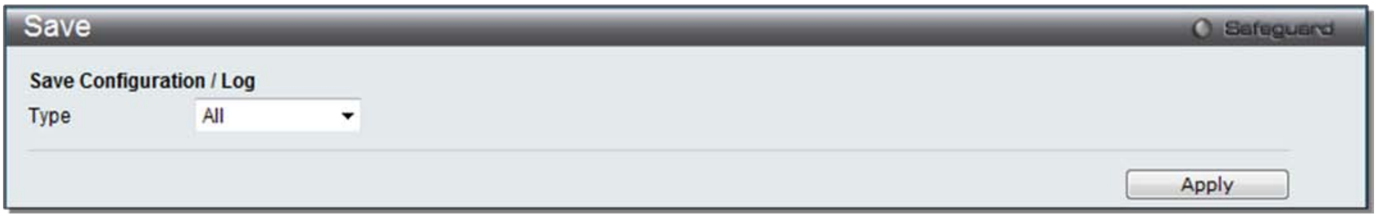
Save Log allows the user to backup the log file of the switch. Select **Log** from the **Type** drop-down menu and click **Apply**.


Save
Safeguard
Save Configuration / Log
Apply

Type Log

Figure 12-2 Save – Log window

Save All allows the user to permanently save changes made to the configuration. This option will allow the changes to be kept after the switch has rebooted. Select **All** from the **Type** drop-down menu and click **Apply**.


Save
Safeguard
Save Configuration / Log
Apply

Type All

Figure 12-3 Save – All window

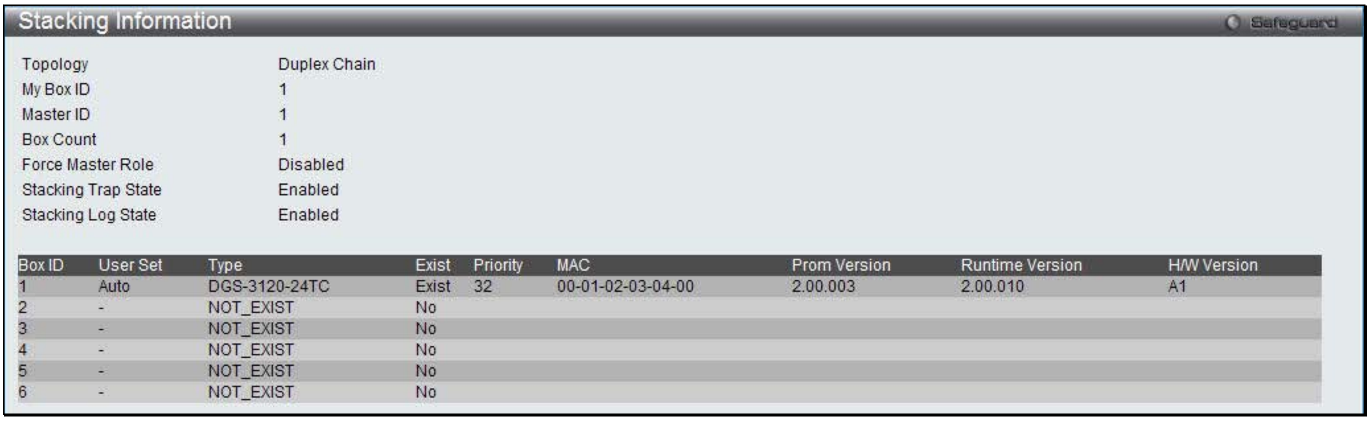
Stacking Information

To change a switch’s default stacking configuration (for example, the order in the stack), see **System Configuration > Stacking > Stacking Mode Settings** window.

The number of switches in the switch stack (up to 6 total) are displayed next to the Tools drop-down menu. The icons are in the same order as their respective Unit numbers, with the Unit 1 switch corresponding to the icon in the upper left-most corner of the icon group.

When the switches are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stacking Information** link.

To view this window, click **Tools > Stacking Information**, as shown below.



Topology Duplex Chain
My Box ID 1
Master ID 1
Box Count 1
Force Master Role Disabled
Stacking Trap State Enabled
Stacking Log State Enabled

Box ID	User Set	Type	Exist	Priority	MAC	Prom Version	Runtime Version	H/W Version
1	Auto	DGS-3120-24TC	Exist	32	00-01-02-03-04-00	2.00.003	2.00.010	A1
2	-	NOT_EXIST	No					
3	-	NOT_EXIST	No					
4	-	NOT_EXIST	No					
5	-	NOT_EXIST	No					
6	-	NOT_EXIST	No					

Figure 12-4 Stacking Information window

The Stacking Information window displays the following information:

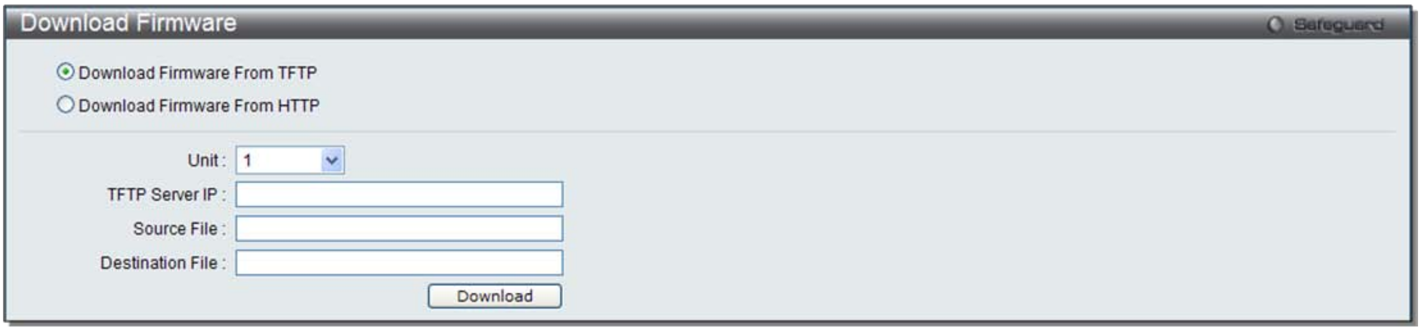
Parameter	Description
Topology	Show the current topology employed using this Switch.
My Box ID	Display the Box ID of the Switch currently in use.
Master ID	Display the Unit ID number of the Primary Master of the Switch stack.
Backup Master	Display the Unit ID of the Backup Master of the switch stack.
Box Count	Display the number of switches in the switch stack.
Box ID	Display the Switch’s order in the stack.
User Set	Box ID can be assigned automatically (Auto), or can be assigned statically. The default is Auto.
Type	Display the model name of the corresponding switch in a stack.
Exist	Denote whether a switch does or does not exist in a stack.
Priority	Display the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack denotes the Primary Master switch.
MAC	Display the MAC address of the corresponding switch in the switch stack.
Prom Version	Show the PROM in use for the Switch. This may be different from the values shown in the illustration.
Runtime Version	Show the firmware version in use for the Switch. This may be different from the values shown in the illustrations.
H/W Version	Show the hardware version in use for the Switch. This may be different from the values shown in the illustration.

Download firmware

The following window is used to download firmware for the Switch.

Download Firmware From TFTP

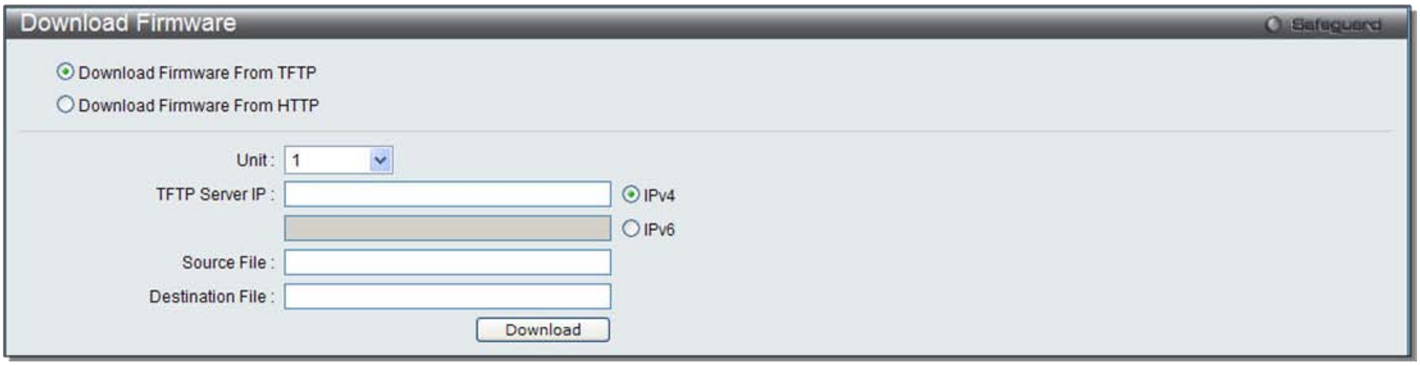
This page allows the user to download firmware from a TFTP Server to the Switch and updates the switch.


Download Firmware
Safeguard
Download Firmware From HTTP
TFTP Server IP :
Source File :
Destination File :
Download

● Download Firmware From TFTP

Unit : 1

Figure 12-5 Download Firmware – TFTP window (SI Mode Only)


Download Firmware
Safeguard
Download Firmware From HTTP
TFTP Server IP :
IPv6
Source File :
Destination File :
Download

● Download Firmware From TFTP

Unit : 1

● IPv4

Figure 12-6 Download Firmware – TFTP window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description	
Unit	Use the drop-down menu to select a unit for receiving the firmware. Select **All** for all units.	
TFTP Server IP	Enter the TFTP server IP address used.	
	IPv4	Click the radio button to enter the TFTP server IP address used.
	IPv6 (EI Mode Only)	Click the radio button to enter the TFTP server IPv6 address used.
Source File	Enter the location and name of the Source File.	
Destination File	Enter the location and name of the Destination File.	

Click **Download** to initiate the download.

Download Firmware From HTTP

This page allows the user to download firmware from a computer to the Switch and updates the switch.

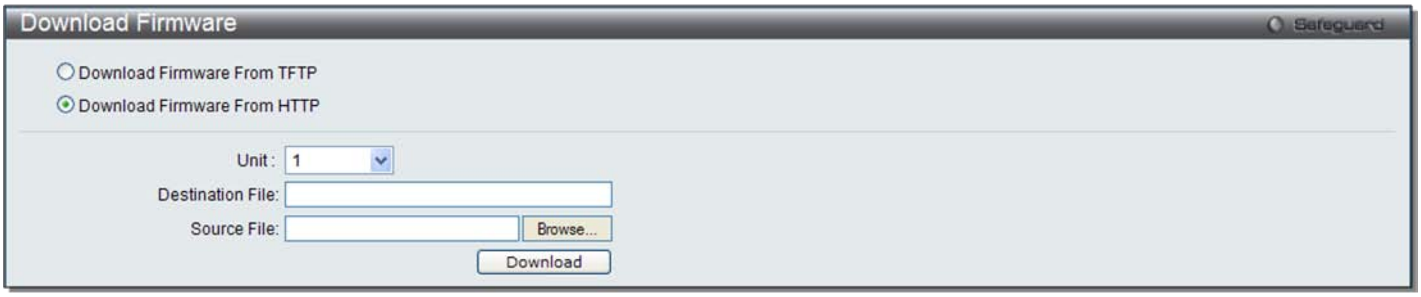

Download Firmware
Safeguard
○ Download Firmware From TFTP
● Download Firmware From HTTP
Unit : 1
Destination File:
Source File:
Browse...
Download

Figure 12-7 Download Firmware – HTTP window

The fields that can be configured are described below:

Parameter	Description
Unit	Use the drop-down menu to select a unit for receiving the firmware. Select **All** for all units.
Destination File	Enter the location of the Destination File.
Source File	Enter the location of the Source File or click the **Browse** button to navigate to the firmware file for the download.

Click **Download** to initiate the download.

Upload Firmware

The following window is used to upload firmware from the Switch.

Upload Firmware To TFTP

This page allows the user to upload firmware from the Switch to a TFTP Server.

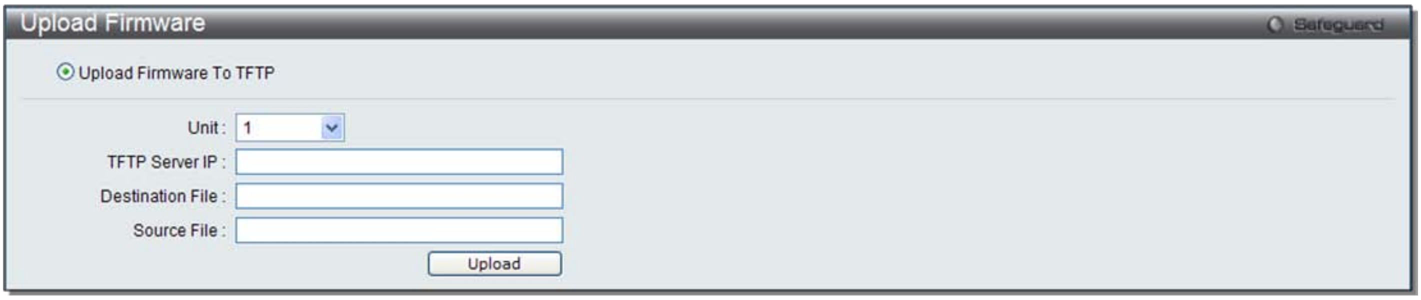

Upload Firmware
Safeguard
● Upload Firmware To TFTP
Unit : 1
TFTP Server IP :
Destination File :
Source File :
Upload

Figure 12-8 Upload Firmware – TFTP window (SI Mode Only)

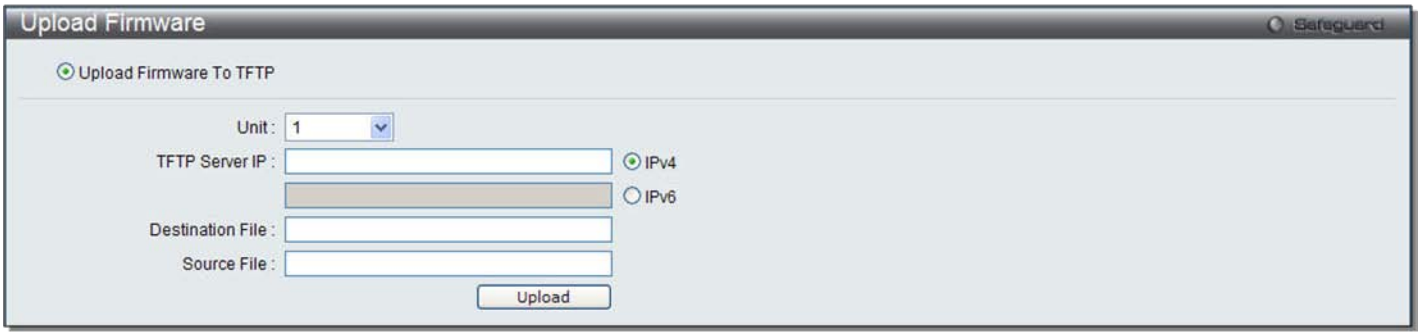

Upload Firmware
Safeguard
● Upload Firmware To TFTP
Unit : 1
TFTP Server IP :
● IPv4
○ IPv6
Destination File :
Source File :
Upload

Figure 12-9 Upload Firmware – TFTP window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description

Unit	Use the drop-down menu to select a unit for uploading the firmware.	
TFTP Server IP	Enter the TFTP server IP address used.	
	IPv4	Click the radio button to enter the TFTP server IP address used.
	IPv6 (EI Mode Only)	Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.	
Source File	Enter the location and name of the Source File.	

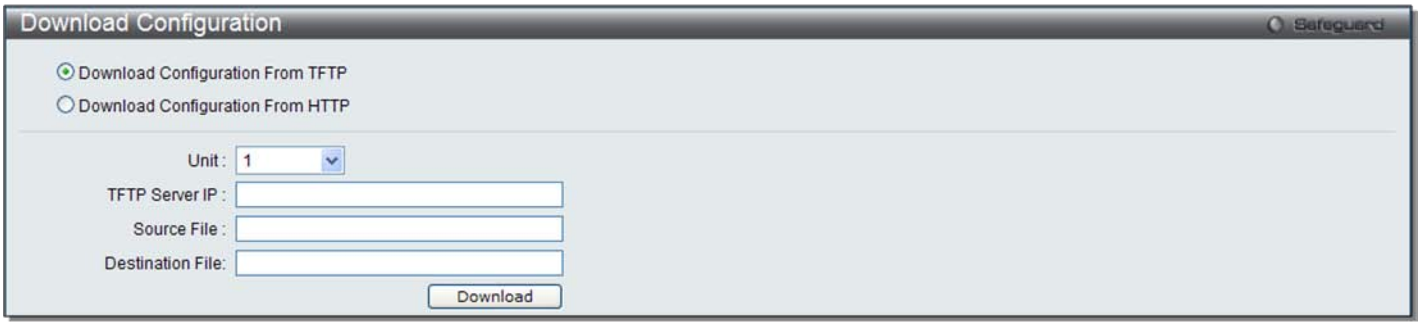
Click **Upload** to initiate the upload.

Download Configuration

The following window is used to download the configuration file for the Switch.

Download Configuration From TFTP

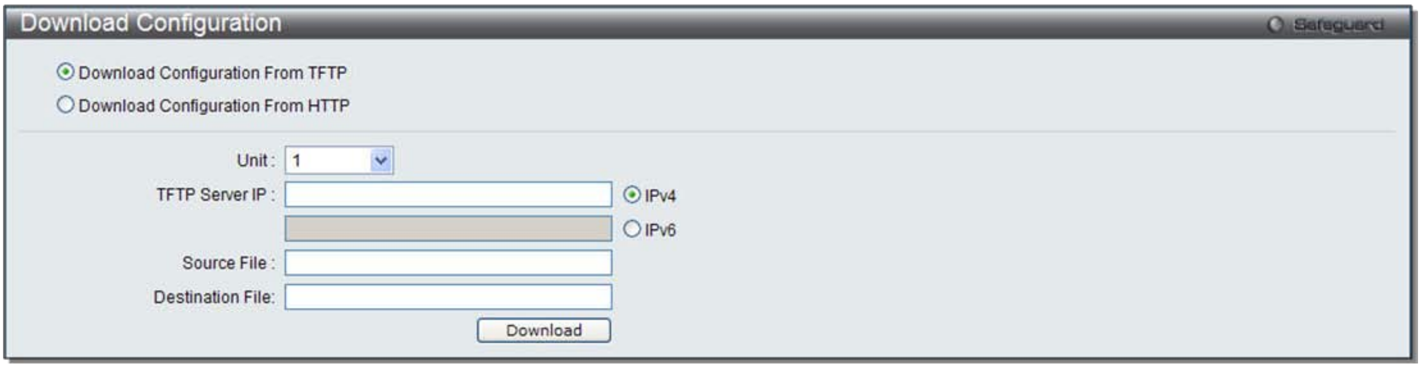
This page allows the user to download the configuration file from a TFTP Server to the Switch and updates the switch.



● Download Configuration From TFTP
○ Download Configuration From HTTP

Unit : 1
TFTP Server IP :
Source File :
Destination File:

Figure 12-10 Download Configuration – TFTP window (SI Mode Only)



● Download Configuration From TFTP
○ Download Configuration From HTTP

Unit : 1
TFTP Server IP : ● IPv4
○ IPv6
Source File :
Destination File:

Figure 12-11 Download Configuration – TFTP window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description	
Unit	Use the drop-down menu to select a unit for receiving the configuration file. Select **All** for all units.	
TFTP Server IP	Enter the TFTP server IP address used.	
	IPv4	Click the radio button to enter the TFTP server IP address used.
	IPv6 (EI Mode Only)	Click the radio button to enter the TFTP server IPv6 address used.

Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File.

Click **Download** to initiate the download.

Download Configuration From HTTP

This page allows the user to download the configuration file from a computer to the Switch and updates the switch.

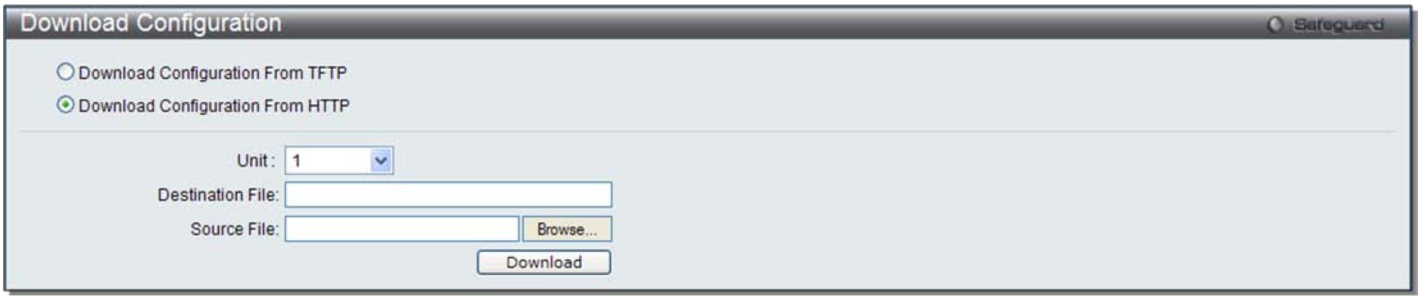

Download Configuration
Safeguard
○ Download Configuration From TFTP
● Download Configuration From HTTP
Unit : 1
Destination File:
Source File:
Browse...
Download

Figure 12-12 Download Configuration – HTTP window

The fields that can be configured are described below:

Parameter	Description
Unit	Use the drop-down menu to select a unit for receiving the configuration file. Select **All** for all units.
Destination File	Enter the location and name of the Destination File.
Source File	Enter the location and name of the Source File, or click the **Browse** button to navigate to the configuration file for the download.

Click **Download** to initiate the download.

Upload Configuration

The following window is used to upload the configuration file from the Switch.

Upload Configuration To TFTP

This page allows the user to upload the configuration file from the Switch to a TFTP Server.

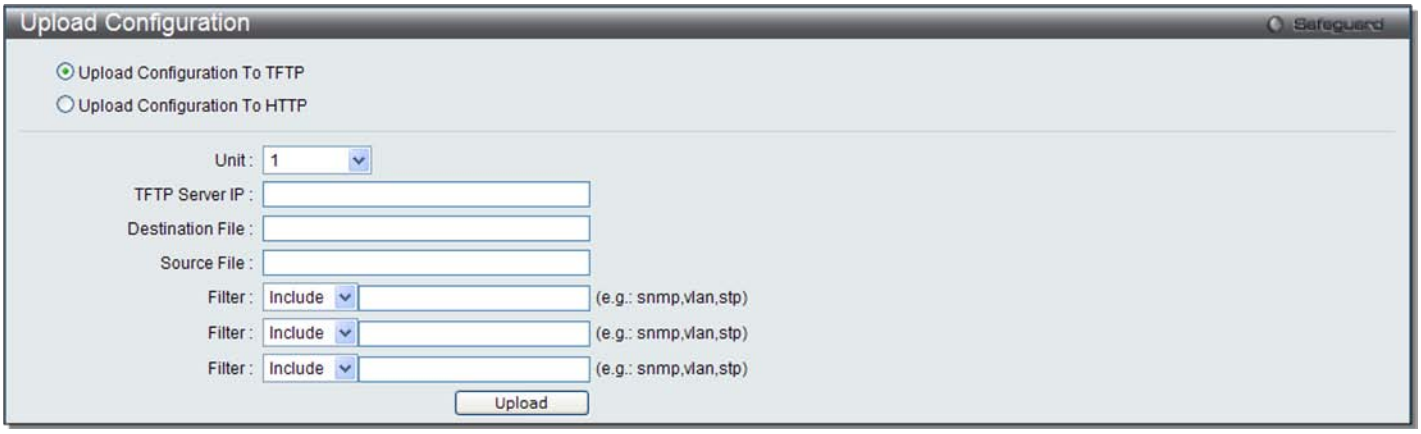

Upload Configuration
Safeguard
● Upload Configuration To TFTP
○ Upload Configuration To HTTP
Unit : 1
TFTP Server IP :
Destination File :
Source File :
Filter : Include (e.g.: snmp,vlan,stp)
Filter : Include (e.g.: snmp,vlan,stp)
Filter : Include (e.g.: snmp,vlan,stp)
Upload

Figure 12-13 Upload Configuration – TFTP window (SI Mode Only)

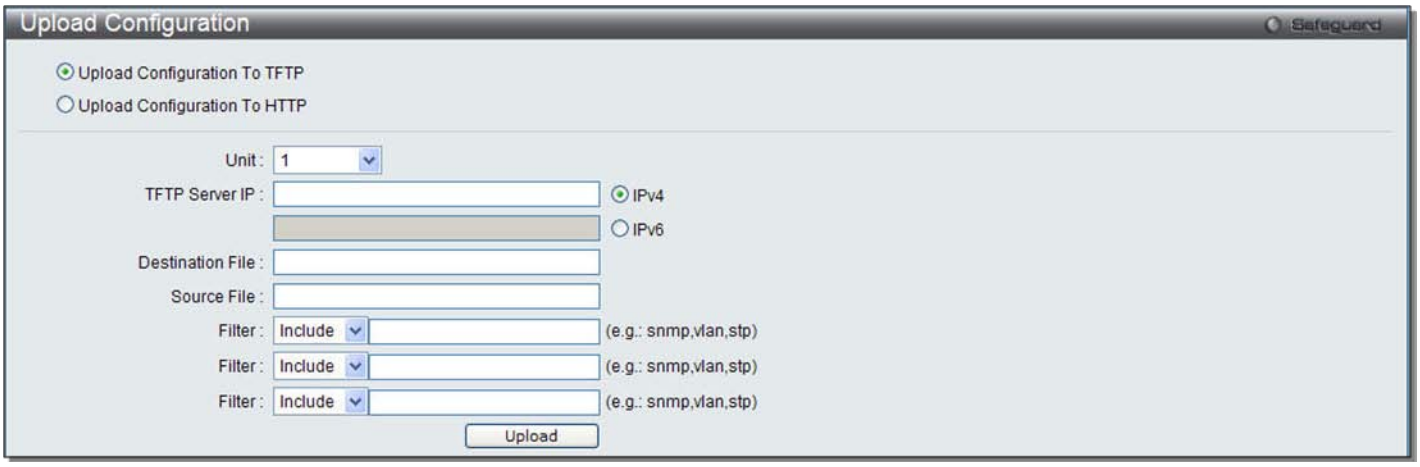

Upload Configuration
Safeguard
● Upload Configuration To TFTP
○ Upload Configuration To HTTP
Unit : 1
TFTP Server IP :
● IPv4
○ IPv6
Destination File :
Source File :
Filter : Include (e.g.: snmp,vlan,stp)
Filter : Include (e.g.: snmp,vlan,stp)
Filter : Include (e.g.: snmp,vlan,stp)
Upload

Figure 12-14 Upload Configuration – TFTP window (EI Mode Only)

The fields that can be configured are described below:

Parameter	Description	
Unit	Use the drop-down menu to select a unit for uploading the configuration file.	
TFTP Server IP	Enter the TFTP server IP address used.	
	IPv4	Click the radio button to enter the TFTP server IP address used.
	IPv6 (EI Mode Only)	Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.	
Source File	Enter the location and name of the Source File.	
Filter	Use the drop-down menu to *include, begin* or *exclude* a filter like SNMP, VLAN or STP. Select the appropriate **Filter** action and enter the service name in the space provided.	

Click **Upload** to initiate the upload.

Upload Configuration To HTTP

This page allows the user to upload the configuration file from the Switch to a computer.

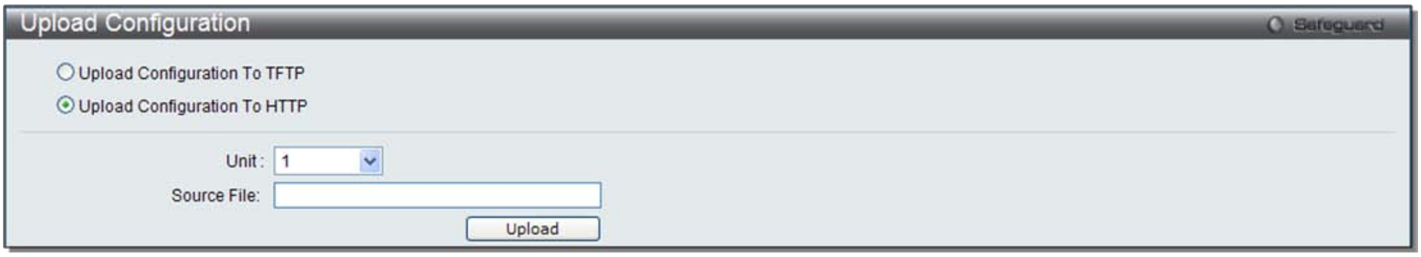

Upload Configuration
Safeguard
○ Upload Configuration To TFTP
● Upload Configuration To HTTP
Unit : 1
Source File:
Upload

Figure 12-15 Upload Configuration – HTTP window

The fields that can be configured are described below:

Parameter	Description
Unit	Use the drop-down menu to select a unit for uploading the configuration file.
Source File	Enter the location and name of the Source File.

Click **Upload** to initiate the upload.

Upload Log File

The following window is used to upload the log file from the Switch.

Upload Log To TFTP

This page allows the user to upload the log file from the Switch to a TFTP Server.

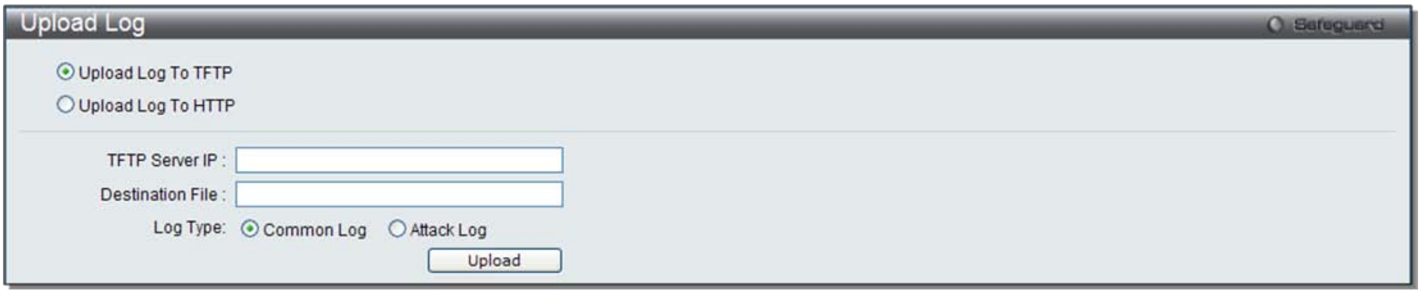

Upload Log
Safeguard
● Upload Log To TFTP
○ Upload Log To HTTP
TFTP Server IP :
Destination File :
Log Type: ● Common Log ○ Attack Log
Upload

Figure 12-16 Upload Log – TFTP window (SI Mode Only)

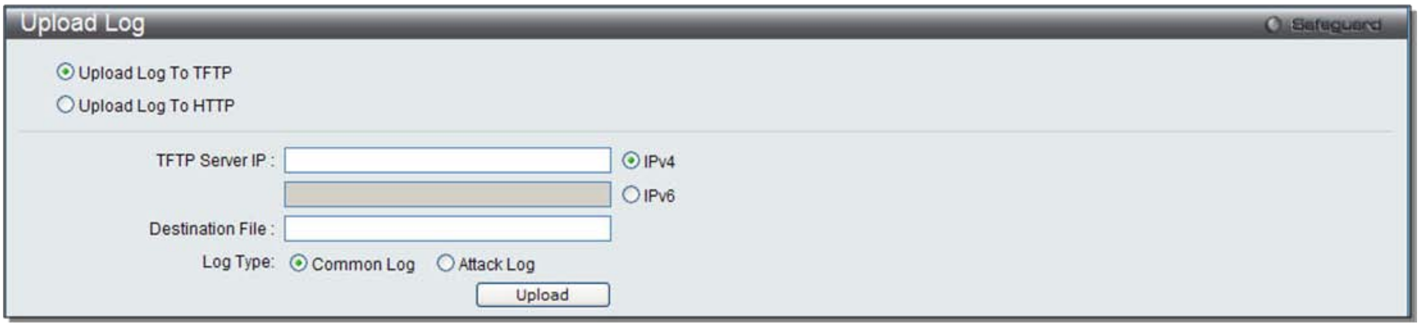

Upload Log
Safeguard
● Upload Log To TFTP
○ Upload Log To HTTP
TFTP Server IP :
● IPv4
○ IPv6
Destination File :
Log Type: ● Common Log ○ Attack Log
Upload

Figure 12-17 Upload Log – TFTP window (EI Mode Only)

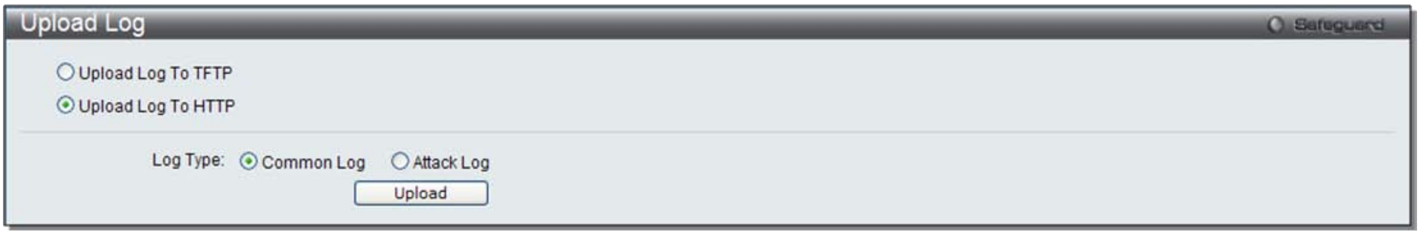
The fields that can be configured are described below:

Parameter	Description	
TFTP Server IP	Enter the TFTP server IP address used.	
	IPv4	Click the radio button to enter the TFTP server IP address used.
	IPv6 (EI Mode Only)	Click the radio button to enter the TFTP server IPv6 address used.
Destination File	Enter the location and name of the Destination File.	
Log Type	Select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.	

Click **Upload** to initiate the upload.

Upload Log To HTTP

This page allows the user to upload the log file from the Switch to a computer.



○ Upload Log To TFTP
● Upload Log To HTTP

Log Type: ● Common Log ○ Attack Log

Figure 12-18 Upload Log – HTTP window

The fields that can be configured are described below:

Parameter	Description
Log Type	Here the user can select the type of log to be transferred. Selecting the **Common Log** option here will upload the common log entries. Selecting the **Attack Log** option here will upload the log concerning attacks.

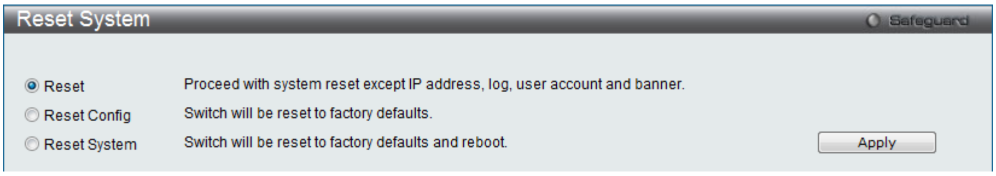
Click **Upload** to initiate the upload.

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.

NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.



● Reset — Proceed with system reset except IP address, log, user account and banner.
○ Reset Config — Switch will be reset to factory defaults.
○ Reset System — Switch will be reset to factory defaults and reboot.

Figure 12-19 Reset System window

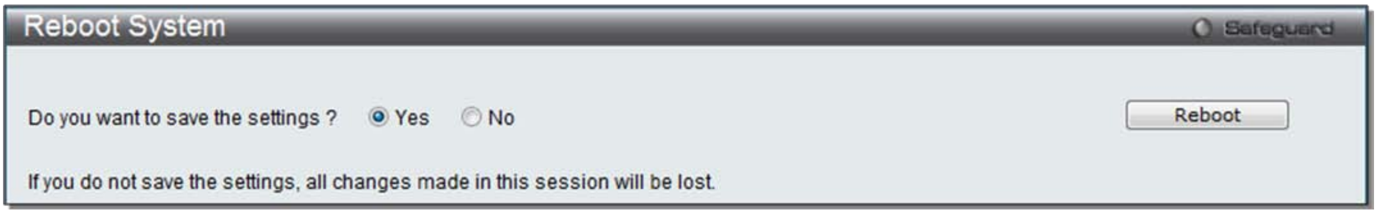
The fields that can be configured are described below:

Parameter	Description
Reset	Selecting this option will factory reset the Switch but not the *IP Address, User Accounts* and the *Banner*.
Reset Config	Selecting this option will factory reset the Switch but not perform a Reboot.
Reset System	Selecting this option will factory reset the Switch and perform a Reboot.

Click the **Apply** button to initiate the Reset action.

Reboot System

The following window is used to restart the Switch.



Do you want to save the settings ? ● Yes ○ No

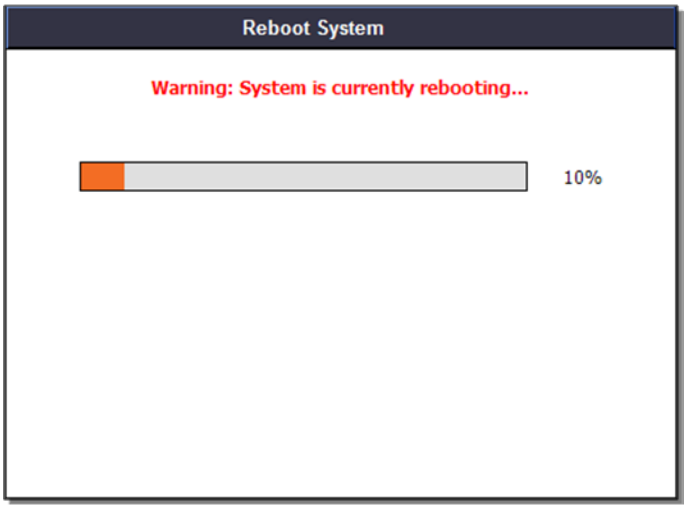
If you do not save the settings, all changes made in this session will be lost.

Figure 12-20 Reboot System Window

Selecting the **Yes** radio button will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Selecting the **No** radio button instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed will be lost.

Click the **Reboot** button to restart the Switch.



Warning: System is currently rebooting...

Figure 12-21 System Rebooting window

Appendix Section

Appendix A Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. However, this protocol is vulnerable because crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce the ARP protocol, ARP spoofing attacks, and the countermeasures brought by D-Link's switches to thwart ARP spoofing attacks.

In the process of ARP, PC A will first issue an ARP request to query PC B's MAC address. The network structure is shown in Figure 1.

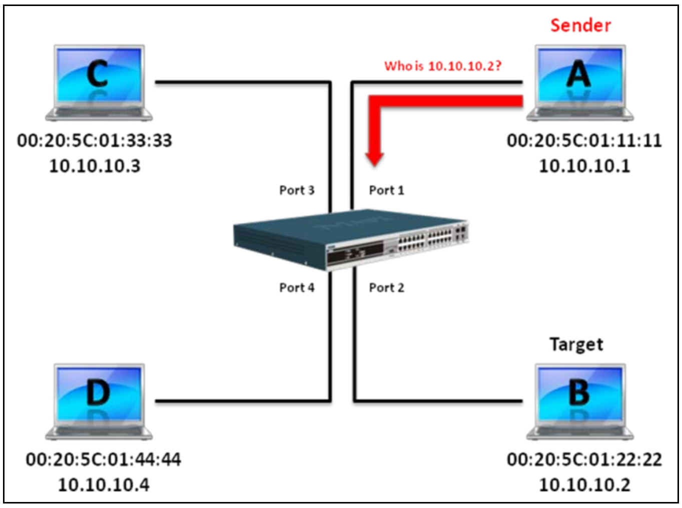
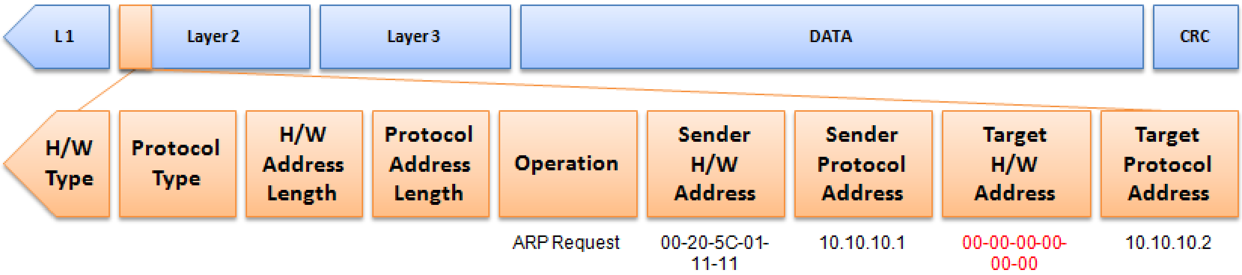

Sender
Who is 10.10.10.2?
C
00:20:5C:01:33:33
10.10.10.3
A
00:20:5C:01:11:11
10.10.10.1
Port 3
Port 1
Port 4
Port 2
Target
D
00:20:5C:01:44:44
10.10.10.4
B
00:20:5C:01:22:22
10.10.10.2

Figure 1

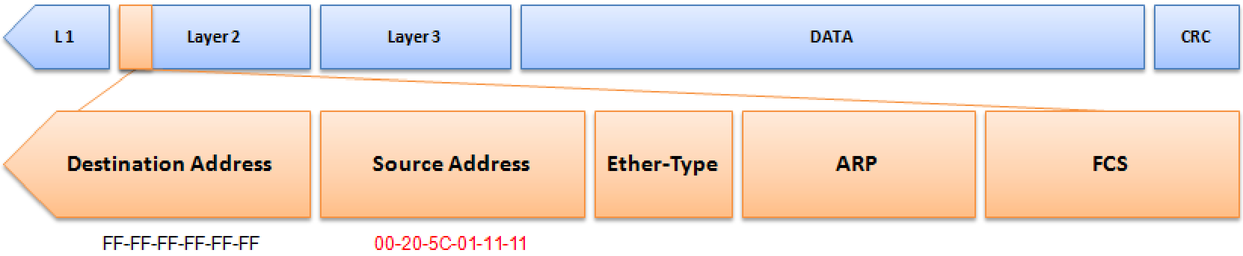
In the meantime, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in the ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00," while PC B's IP address will be written into the "Target Protocol Address," shown in Table1.


L1
Layer 2
Layer 3
DATA
CRC

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP Request	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

Table 1 ARP Payload

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Table 2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via broadcast, the "Destination address" is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).


L1
Layer 2
Layer 3
DATA
CRC

Destination Address	Source Address	Ether-Type	ARP	FCS
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11			

Table 2 Ethernet Frame Format

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.

Forwarding Table:
Port 1 : 00-20-5C-01-11-11

In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 2).

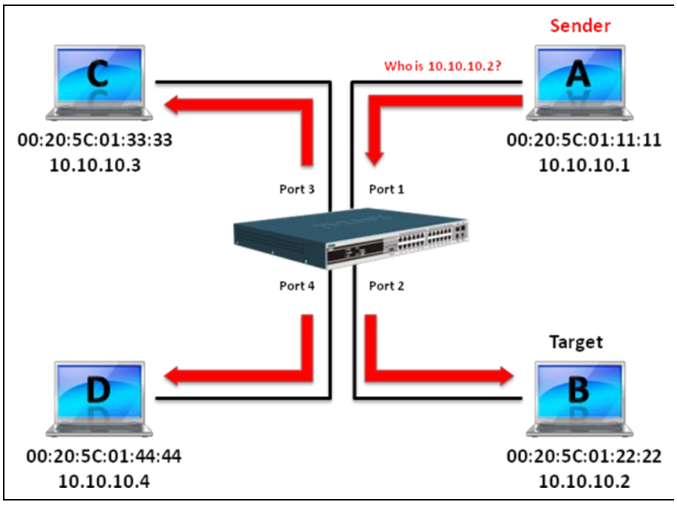

Sender
Who is 10.10.10.2?
C
A
00:20:5C:01:33:33
10.10.10.3
00:20:5C:01:11:11
10.10.10.1
Port 3
Port 1
Port 4
Port 2
Target
D
B
00:20:5C:01:44:44
10.10.10.4
00:20:5C:01:22:22
10.10.10.2

Figure 2

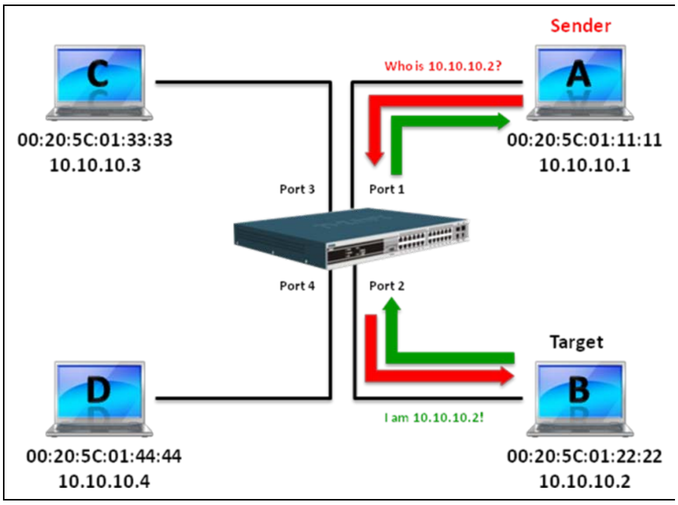
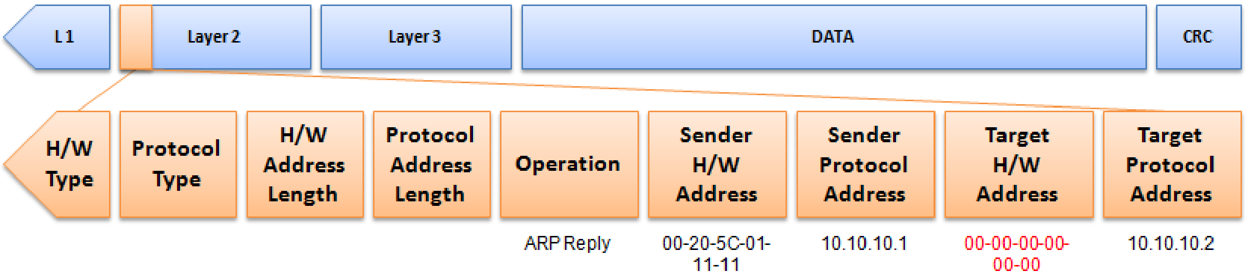

Sender
Who is 10.10.10.2?
C
A
00:20:5C:01:33:33
10.10.10.3
00:20:5C:01:11:11
10.10.10.1
Port 3
Port 1
Port 4
Port 2
Target
D
B
I am 10.10.10.2!
00:20:5C:01:44:44
10.10.10.4
00:20:5C:01:22:22
10.10.10.2

Figure 3

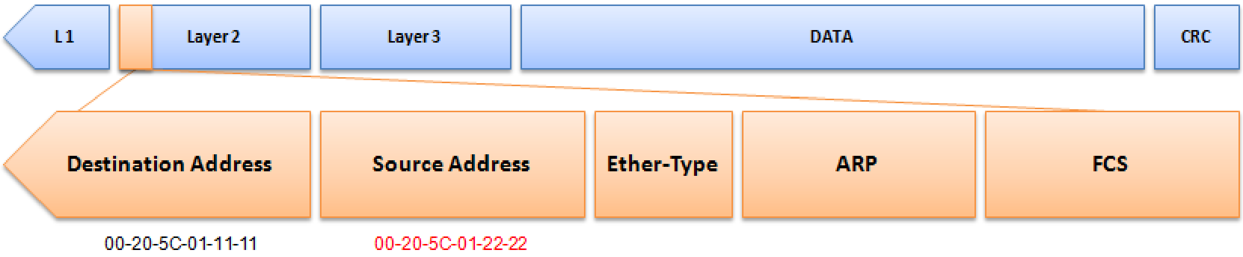
When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table 3. The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.


L1
Layer 2
Layer 3
DATA
CRC

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP Reply	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

Table 3 ARP Payload

When PC B replies to the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table 4).


L1
Layer 2
Layer 3
DATA
CRC

Destination Address	Source Address	Ether-Type	ARP	FCS
00-20-5C-01-11-11	00-20-5C-01-22-22			

Table 4 Ethernet Frame Format

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table:
Port 1 : 00-20-5C-01-11-11
Port 2 : 00-20-5C-01-22-22

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

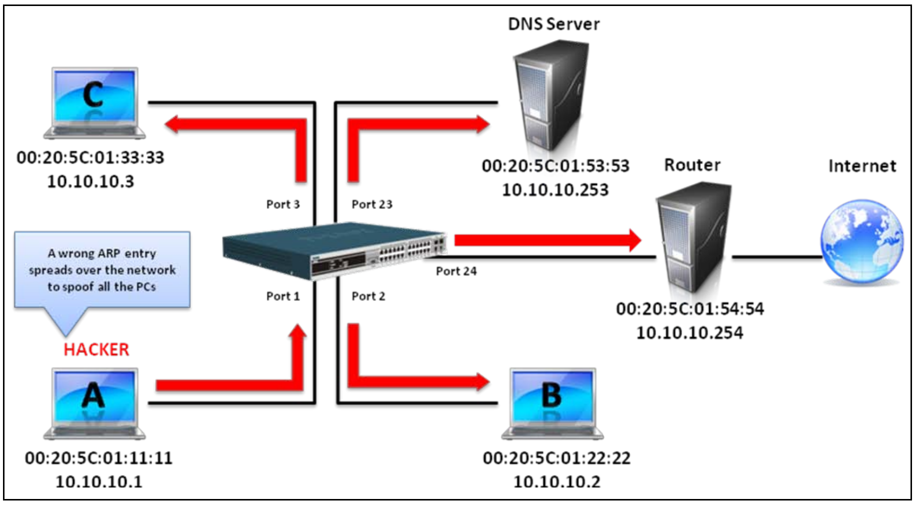
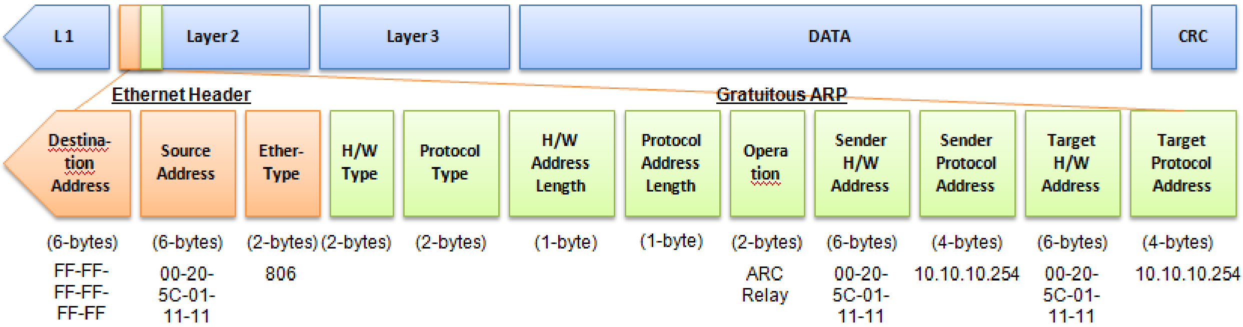

DNS Server
C
00:20:5C:01:33:33
10.10.10.3
00:20:5C:01:53:53
10.10.10.253
Router
Internet
Port 3
Port 23
A wrong ARP entry spreads over the network to spoof all the PCs
Port 24
Port 1
Port 2
00:20:5C:01:54:54
10.10.10.254
HACKER
A
B
00:20:5C:01:11:11
10.10.10.1
00:20:5C:01:22:22
10.10.10.2

Figure 4

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in the following table.


L1
Layer 2
Layer 3
DATA
CRC

Ethernet Header			Gratuitous ARP								
Destination Address	Source Address	Ether-Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-bytes)	(6-bytes)	(2-bytes)	(2-bytes)	(2-bytes)	(1-byte)	(1-byte)	(2-bytes)	(6-bytes)	(4-bytes)	(6-bytes)	(4-bytes)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	806					ARC Relay	00-20-5C-01-11-11	10.10.10.254	00-20-5C-01-11-11	10.10.10.254

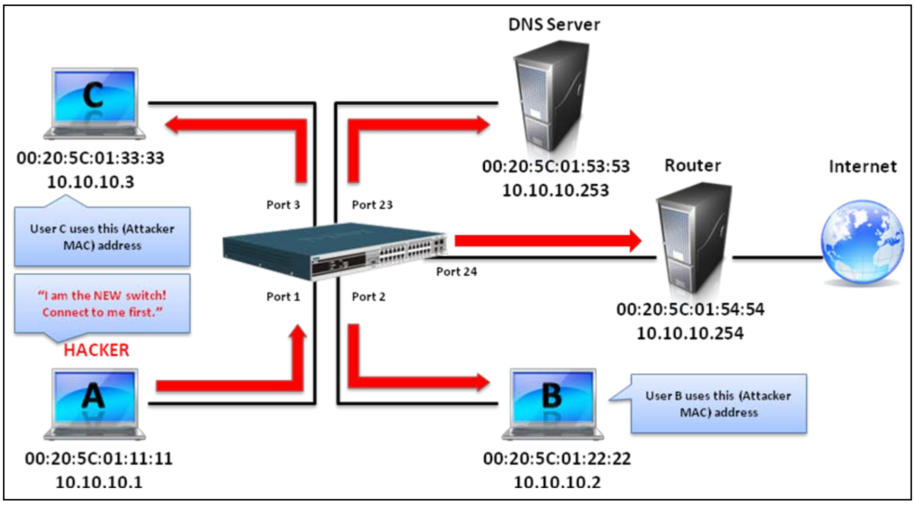

DNS Server
C
00:20:5C:01:33:33
10.10.10.3
User C uses this (Attacker MAC) address
"I am the NEW switch! Connect to me first."
HACKER
A
00:20:5C:01:11:11
10.10.10.1
Port 3
Port 23
Port 1
Port 2
Port 24
00:20:5C:01:53:53
10.10.10.253
Router
Internet
00:20:5C:01:54:54
10.10.10.254
B
00:20:5C:01:22:22
10.10.10.2
User B uses this (Attacker MAC) address

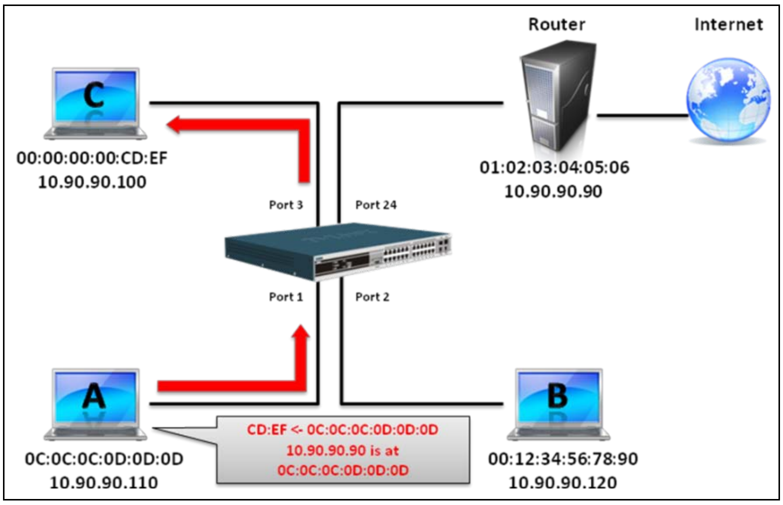
Figure 5

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack).

The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 5 all traffic will be then sniffed by the hacker but the users will not discover.

Prevent ARP Spoofing via Packet Content ACL


Router
Internet
C
00:00:00:00:CD:EF
10.90.90.100
01:02:03:04:05:06
10.90.90.90
Port 3
Port 24
Port 1
Port 2
A
0C:0C:0C:0D:0D:0D
10.90.90.110
CD:EF <- 0C:0C:0C:0D:0D:0D
10.90.90.90 is at
0C:0C:0C:0D:0D:0D
B
00:12:34:56:78:90
10.90.90.120

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL on the Switch to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

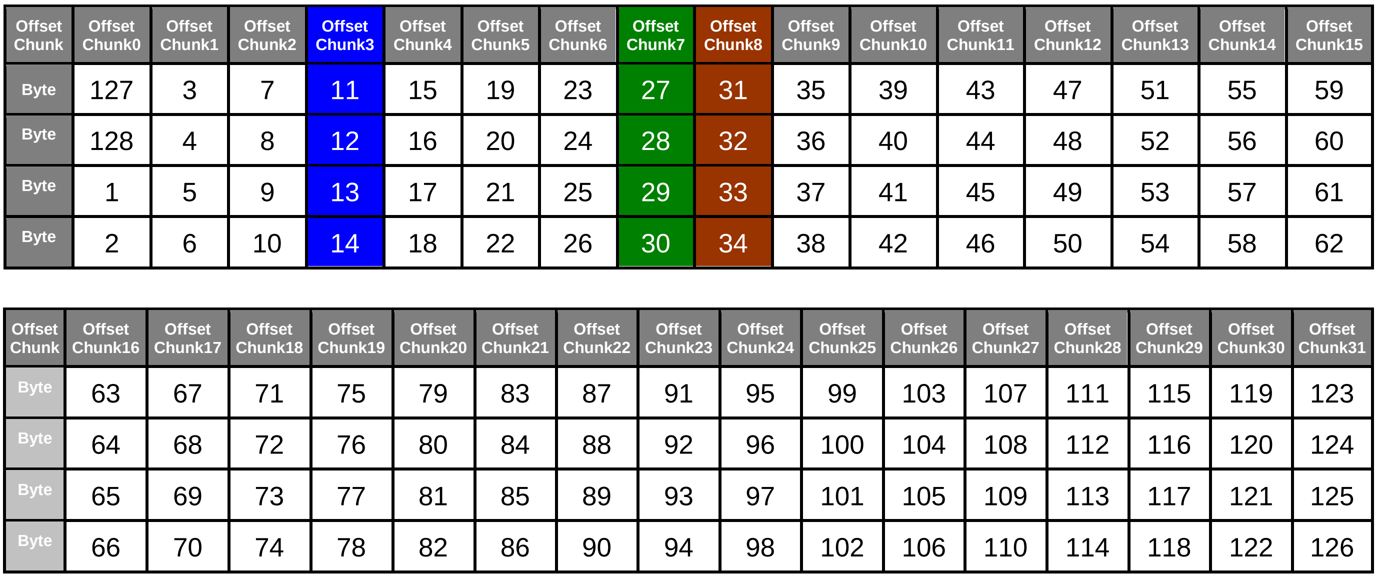
Configuration

The configuration logic is as follows:

1. Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on the Switch enables users to inspect any offset chunk. An offset chunk is a 4-byte block in a HEX format, which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset chunks can be applied to each profile and a switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset chunks.

In Table 6, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset chunk is scratched from 1 but not zero.



Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table 6. Chunk and Packet Offset

The following table indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

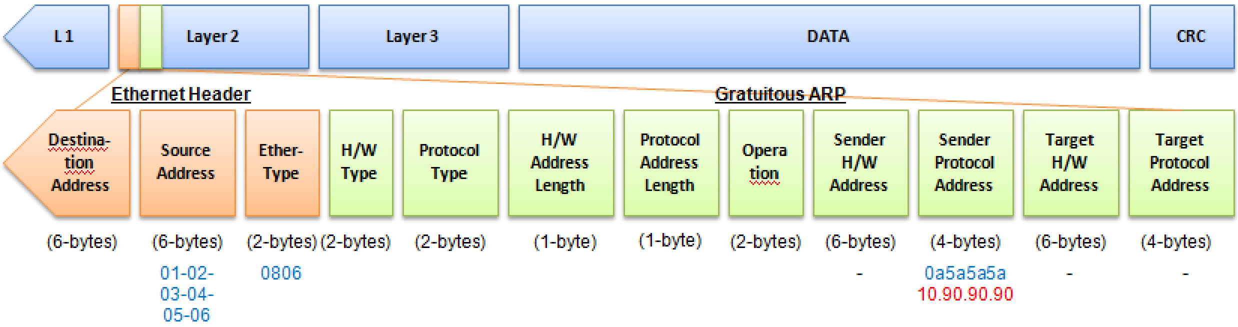

L1
Layer 2
Layer 3
DATA
CRC
Ethernet Header
Gratuitous ARP
Destination Address
Source Address
Ether-Type
H/W Type
Protocol Type
H/W Address Length
Protocol Address Length
Operation
Sender H/W Address
Sender Protocol Address
Target H/W Address
Target Protocol Address
(6-bytes)
(6-bytes)
(2-bytes)
(2-bytes)
(2-bytes)
(1-byte)
(1-byte)
(2-bytes)
(6-bytes)
(4-bytes)
(6-bytes)
(4-bytes)
01-02-03-04-05-06
0806
-
0a5a5a5a
10.90.90.90
-
-

Table 5 A Completed ARP Packet Contained in an Ethernet Frame

	Command	Description
Step 1:	`create access_profile_id 1 profile_name 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type`	Create access profile 1 to match Ethernet Type and Source MAC address.
Step 2:	`config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit`	Configure access profile 1 Only if the gateway's ARP packet that contains the correct Source MAC in the Ethernet frame can pass through the switch.

Step 3:	`create access_profile profile_id 2 profile_name 2 packet_content_mask`
	`offset_chunk_1 3 0xFFFF`
	`offset_chunk_2 7 0xFFFF`
	`offset_chunk_3 8 0xFFFF0000`
		Create access profile 2
		The first chunk starts from Chunk 3 mask for Ethernet Type. (Blue in Table 6, 13th and 14th bytes)
		The second chunk starts from Chunk 7 mask for Sender IP in ARP packet. (Green in Table 6, 29th and 30th bytes)
		The third chunk starts from Chunk 8 mask for Sender IP in ARP packet. (Brown in Table 6, 31st and 32nd bytes)

Step 4:	`config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x806 offset_chunk_2`	Configure access profile 2. The rest of the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.

	`0xA5A offset_chunk_3 0x5A5A0000`	
Step 5:	`save`	Save configuration.

Appendix B Password Recovery Procedure

This document describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This document will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the Switch. After the UART init is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled.

```
Boot Procedure                                                     V2.00.003
-------------------------------------------------------------------------------


  Power On Self Test ........................................  100%

  MAC Address   : 00-01-02-03-04-00
  H/W Version   : A1

   Please Wait, Loading V2.00.010 Runtime Image .............  100 %
.  UART init .................................................  100 %
```

```
Password Recovery Mode
>
```

1. In the “Password Recovery Mode” only the following commands can be used.

Command	Parameters
reset config {force_agree}	The **reset config** command resets the whole configuration back to the default values. The option '**force_agree**' means to reset the whole configuration without the user’s agreement.
reboot	The **reboot** command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix C System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
System	System started up	[Unit <unitID>,] System started up	Critical	
	System warm start	[Unit <unitID>,] System warm start	Critical	
	System cold start	[Unit <unitID>,] System cold start	Critical	
	Configuration saved to flash	[Unit <unitID>,] Configuration saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	System log saved to flash	[Unit <unitID>,] System log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration and log saved to flash	[Unit <unitID>,] Configuration and log saved to flash by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Internal Power failed	[Unit <unitID>,] Internal Power failed	Critical	
	Internal Power is recovered	[Unit <unitID>,] Internal Power is recovered	Critical	
	Redundant Power failed	[Unit <unitID>,] Redundant Power failed	Critical	
	Redundant Power is working	[Unit <unitID>,] Redundant Power is working	Critical	
	Side Fan failed	[Unit <unitID>,] Side Fan failed	Critical	
	Side Fan recovered	[Unit <unitID>,]Side Fan recovered	Critical	
up/down-load	Firmware upgraded successfully	[Unit <unitID>,] Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Firmware upgrade was unsuccessful	[Unit <unitID>,] Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration successfully downloaded	Configuration successfully downloaded by console(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string,

				which means if user login by console, there will no IP information for logging.
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Configuration upload was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Firmware successfully uploaded	Firmware successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Firmware upload was unsuccessful	Firmware upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
Interface	Port link up	Port <[unitID:]portNum> link up, <link state>	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	Port <[unitID:]portNum> link down	Informational	
Stacking	Hot insert	Unit<UnitID>,MAC:<macaddr> Hot insertion.	Informational	
	Hot remove	Unit<UnitID>,MAC:<macaddr> Hot removal.	Informational	
	Firmware upgraded to SLAVE successfully	Firmware upgraded to SLAVE successfully (Username:<username>)	Informational	
	Firmware upgraded to SLAVE unsuccessfully	Firmware upgraded to SLAVE unsuccessfully! (Username: <username>)	Warning	
	Stacking topology change.	Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>)	Informational	
	Backup master changed to master	Backup master changed to master. Master (Unit: <unitID>)	Informational	
	Slave changed to master	Slave changed to master. Master (Unit: <unitID>)	Informational	
	Box ID conflict	Hot insert failed, box ID conflict: Unit	Critical	

		<unitID> conflict (MAC: <macaddr> and MAC: <macaddr>)		
Console	Successful login through Console	[Unit <unitID>,] Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console	[Unit <unitID>,] Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Logout through Console	[Unit <unitID>,] Logout through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Console session timed out	[Unit <unitID>,] Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Web session timed out	Web session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	Successful login through Web(SSL)	Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web(SSL)	Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web(SSL)	Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Web(SSL) session timed out	Web(SSL) session timed out (Username: <username>, IP: <ipaddr>)	Informational	
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational	
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational	
STP	Topology changed	Topology changed (Instance:<InstanceID> ,Port:<[unitID:]portNum>,MAC:<macaddr>)	Informational	
	New Root selected	[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>)	Informational	
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational	
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational	
	New root port	New root port selected (Instance:<InstanceID>, port:<[unitID:]portNum>)	Notice	
	Spanning Tree port status changed	Spanning Tree port status change (Instance:<InstanceID> , Port:<[unitID:]portNum>) <old_status> -> <new_status>	Notice	
	Spanning Tree port role changed	Spanning Tree port role change (Instance:<InstanceID> , Port:<unitID:portNum>) <old_role> -> <new_role>	Informational	
	Spannnig Tree instance created	Spanning Tree instance created (Instance:<InstanceID>)	Informational	
	Spannnig Tree instance deleted	Spanning Tree instance deleted (Instance:<InstanceID>)	Informational	
	Spanning Tree Version changed	Spanning Tree version change (new version:<new_version>)	Informational	
	Spanning Tree MST configuration ID name and revision level changed	Spanning Tree MST configuration ID name and revision level change	Informational	

		(name:<name> ,revision level <revision_level>).		
	Spanning Tree MST configuration ID VLAN mapping table deleted	Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [-<endvlanid>])	Informational	
	Spanning Tree MST configuration ID VLAN mapping table added	Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>])	Informational	
DoS	Spoofing attack 1. The soure ip is same as switch's interface ip but the source mac is different 2. Source ip is the same as the switch's IP in ARP packet 3. Self IP packet detected	Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>	Informational	
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>,)	Warning	
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	SSH server is enabled	SSH server is enabled	Informational	
	SSH server is disabled	SSH server is disabled	Informational	
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational	
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational	
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web(SSL) authenticated by AAA local method	Successful login through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web(SSL) authenticated by AAA local method	Login failed through Web(SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>,)	Informational	
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web(SSL) authenticated by AAA none method	Successful login through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	

	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web(SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web(SSL) authenticated by AAA server	Login failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web(SSL) due to AAA server timeout or improper configuration	Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through SSH due to AAA server timeout or improper configuration	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method	Informational	

		(Username: <username>,)		
	Enable Admin failed through Web(SSL) authenticated by AAA local_enable method	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through <Telnet or Web or SSH> from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web(SSL) authenticated by AAA none method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA server	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web(SSL) authenticated by AAA server	Enable Admin failed through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username:	Informational	

		<username>)		
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
Port Security	port security is exceeded to its maximum learning size and will not learn any new address	Port security violation (MAC address: <macaddr> on port: <[unitID:]portNum>)	Warning	
RADIUS	VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member.	RADIUS server <ipaddr> assigned VID :<vlanID> to port <[unitID:]portNum> (account :<username>)	Informational	
	Ingress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port.	RADIUS server <ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <[unitID:]portNum> (account : <username>)	Informational	
	Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This egress bandwidth will be assigned to the port.	RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <[unitID:]portNum> (account: <username>)	Informational	
	802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port.	RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <[unitID:]portNum> (account : <username>)	Informational	
	Failed to assign ACL profiles/rules from RADIUS server.	RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID]portNum> (<string>)	Warning	
802.1X	802.1X Authentication failure.	802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)	Warning	
	802.1X Authentication successful.	802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>)	Informational	
MAC-based Access Control	A host fails to pass the authentication	MAC-based Access Control unauthenticated host(MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)	Critical	
	The authorized user number on a port reaches the max user limit.	Port <[unitID:]portNum> enters MAC-based Access Control stop learning state.	Warning	per port
	The authorized user number on a port is below the max user limit in a time interval(interval is project depended).	Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state.	Warning	per port
	The authorized user number on whole device reaches the max user limit.	MAC-based Access Control enters stop learning state.	Warning	per system
	The authorized user number on whole device is below the max user limit in a time interval(interval is project depended).	MAC-based Access Control recovers from stop learning state.	Warning	per system
	A host passes the authentication	MAC-based Access Control host login successful (MAC: <macaddr>, port:	Informational	

		<[unitID]portNum>, VID: <vid>)		
	A host is aged out	MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID]portNum>, VID: <vid>)	Informational	
JWAC	When a client host authenticated successful.	JWAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)	Informational	
	When a client host fails to authenticate.	JWAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning	
	This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device.	JWAC enters stop learning state.	Warning	per system
	This log will be triggered when the number of authorized users is below the maximum user limit on whole device in 5 minutes	JWAC recovers from stop learning state.	Warning	per system
WAC	When a client host authenticated successful.	WAC authenticated user (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>)	Informational	
	When a client host fails to authenticate.	WAC unauthenticated user (User Name: <string>, IP: <ipaddr | ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning	
	The authorized user number on whole device reaches the max user limit.	WAC enters stop learning state.	Warning	per system
	The authorized user number on whole device is below the max user limit in a time interval(interval is project depended).	WAC recovers from stop learning state.	Warning	per system
IMPB	Unauthenticated IP address encountered and discarded by IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IMPB (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry conflicts with static FDB(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry conflicts with static IMPB(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
	Creating IMPB entry failed due to no ACL rule available	Creating IMPB entry failed due to no ACL rule being available(IP:<ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
IP and Password Changed	IP Address change activity	[Unit <unitID>,] Management IP address was changed by console(Username: <username>,IP:<ipaddr>)	Informational	"console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
	Password change activity	[Unit <unitID>,] Password was changed by console (Username: <username>,IP:<ipaddr>)	Informational	"console" and "IP: <ipaddr>" are XOR shown in log string, which means if user login by console, there will no IP information for logging.
Safeguard Engine	Safeguard Engine is in normal mode	[Unit <unitID>] Safeguard Engine enters NORMAL mode	Informational	
	Safeguard Engine is in filtering packet mode	[Unit <unitID>] Safeguard Engine enters EXHAUSTED mode	Warning	
Packet Storm	Broadcast strom occurrence	Port <[unitID:]portNum> Broadcast storm	Warning	

		is occurring		
	Broadcast storm cleared	Port <[unitID:]portNum> Broadcast storm has cleared	Informational	
	Multicast storm occurrence	Port <[unitID:]portNum> Multicast storm is occurring	Warning	
	Multicast storm cleared	Port <[unitID:]portNum> Multicast storm has cleared	Informational	
	Port shut down due to a packet storm	Port <[unitID:]portNum> is currently shut down due to a packet storm	Warning	
Loop Back Dection	Port loop occurred	Port <[unitID:]portNum> LBD loop occurred. Port blocked	Critical	
	Port loop detection restarted after interval time	Port <[unitID:]portNum> LBD port recovered. Loop detection restarted	Informational	
	Port with VID loop occurred	Port <[unitID:]portNum> VID <vlanID> LBD loop occurred. Packet discard begun	Critical	
	Port with VID Loop detection restarted after interval time	Port <[unitID:]portNum> VID <vlanID> LBD recovered. Loop detection restarted	Informational	
	The number of VLANs that loop back has occured hit the specified number.	Loop VLAN number overflow	Informational	
Gratuituios ARP	Gratuituios ARP detected duplicate IP.	Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>).	Warning	
DHCP	Detect untrusted DHCP server IP address	Detected untrusted DHCP server(IP: <ipaddr>, Port: <[unitID:]portNum>)	Informational	DHCP Server Screening
BPDU Protection	BPDU attack happened	Port <[UnitID:]portNum> enter BPDU under attacking state (mode: drop / block / shutdown)	Informational	
	BPDU attack automatically recover	Port <[UnitID:]portNum> recover from BPDU under attacking state automatically	Informational	
	BPDU attack manually recover	Port <[UnitID:]portNum> recover from BPDU under attacking state manually	Informational	
MONITOR	Temperature exceeds confidence level	[Uint <unitID>] Temperature Sensor <sensorID> enter alarm state. (current temperature: <temperature>)	Warning	
	Temperature recovers to normal.	[Uint <unitID>] Temperature Sensor <sensorID> recovers to normal state. (current temperature: <temperature>)	Informational	
CFM	Cross-connect is detected	CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Critical	
	Error CFM CCM packet is detected	CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)	Warning	
	Can not receive remote MEP's CCM packet	CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Warning	
	Remote MEP's MAC reports an error status	CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Warning	
	Remote MEP detects CFM defects	CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>)	Informational	
CFM EXTENSION	AIS condition detected	AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	

	AIS condition cleared	AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK condition detected	LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
	LCK condition cleared	LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>)	Notice	
Voice VLAN	When a new voice device is detected in the port	New voice device detected (MAC:<macaddr>,Port:<[unitID:]portNum>)	Informational	
	While the port join to the voice VLAN while the port is auto voice VLAN mode	Port <[unitID:]portNum> add into voice VLAN <vid >	Informational	
	While the port withdraws from the voice VLAN while there is no more voice device detected in the aging interval.	Port <[unitID:]portNum> remove from voice VLAN <vid >	Informational	
ERPS	Signal failure detected	Signal failure detected on node <macaddr>	Notice	
	Signal failure cleared	Signal failure cleared on node <macaddr>	Notice	
	RPL owner conflict	RPL owner conflicted on the ring <macaddr>	Warning	
Command logging	Command Logging	<username>: execute command "<string>".	Informational	
LAC	Lac trunk group link down and link up log.	Link aggregation Group <LAG Index> (Interface: <LAG interface index>) <link status>	Information	
SD Card Management	Execute configuration error.	Error when execute configuration <filename> line:<lineno> at time < time-range>.	Warning	
	Schedule backup fail.	Backup <type>:<filename> at time <time-range> failure.	Warning	
	Execute configuration success.	Execute configuration <filename> success at time < time-range>.	Informational	
	Schedule backup success.	Backup <type>:<filename> success at time <time-range>.	Informational	
LLDP	LLDP-MED Topology change detected	LLDP-MED Topology change detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	
	Conflict LLDP-MED device type detected	Conflict LLDP-MED device type detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	
	Incompatible LLDP-MED TLV set detected	Incompatible LLDP-MED TLV set detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	

Appendix D Trap Log Entries

This table lists the trap logs found on the Switch.

Log Entry	Description	OID
swL2macNotification	This trap indicate the MAC addresses variation in the address table. Binding 1: swL2macNotifyInfo	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.1 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.1 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.1 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.1 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.1 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.1 (DGS-3120-24SC-DC)
swL2PortSecurityViolationTrap	When the port_security trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out. Binding 1: swL2PortSecurityPortIndex 2: swL2PortSecurityViolationMac	1.3.6.1.4.1.171.11.117.1.1.2.100.1.2.0.2 (DGS-3120-24TC) 1.3.6.1.4.1.171.11.117.1.2.2.100.1.2.0.2 (DGS-3120-24PC) 1.3.6.1.4.1.171.11.117.1.3.2.100.1.2.0.2 (DGS-3120-24SC) 1.3.6.1.4.1.171.11.117.1.4.2.100.1.2.0.2 (DGS-3120-48TC) 1.3.6.1.4.1.171.11.117.1.5.2.100.1.2.0.2 (DGS-3120-48PC) 1.3.6.1.4.1.171.11.117.1.6.2.100.1.2.0.2 (DGS-3120-24SC-DC)
swIpMacBindingViolationTrap	When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out. Binding 1: swIpMacBindingPortIndex 2: swIpMacBindingViolationIP 3: swIpMacBindingViolationMac	1.3.6.1.4.1.171.12.23.5.0.1
swL2IpMacBindingStopLearningTrap	When the IP-MAC Binding trap is enabled, if the specific port changes from a normal state to a stop_learning state, a trap will be sent out. Binding 1:swL2IpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.2
swL2IpMacBindingRecoverLearningTrap	When the IP-MAC Binding trap is enabled, if the specific port changes from a stop_learning state to a normal state, a trap will be sent out. Binding 1:swL2IpMacBindingPortIndex	1.3.6.1.4.1.171.12.23.5.0.3
swPktStormOccurred	The trap is sent when packet storm is detected by packet storm mechanism and take shutdown as action. Binding 1: swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.1
swPktStormCleared	The trap is sent when the packet storm is cleared by packet storm mechanism. Binding 1: swPktStormCtrlPortIndex	1.3.6.1.4.1.171.12.25.5.0.2
SafeGuardChgToExhausted	This trap indicates System change operation mode from normal to exhausted.	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	This trap indicates System change operation mode from exhausted to normal.	1.3.6.1.4.1.171.12.19.4.1.0.2
agentGratuitousARPTrap	This trap is sent when there is an IP address conflict. Binding 1. agentGratuitousARPIpAddr 2. agentGratuitousARPMacAddr 3. agentGratuitousARPPortNumber 4. agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.12.1.7.2.0.5
swMacBasedAccessControlLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.1

swMacBasedAccessControlLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.2
swMacBasedAccessControlAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding 1. swMacBasedAuthInfoMacIndex 2. swMacBasedAuthInfoPortIndex 3. swMacBasedAuthVID	1.3.6.1.4.1.171.12.35.11.1.0.3
swFilterDetectedTrap	Send trap when illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration. Binding 1. swFilterDetectedIP 2. swFilterDetectedport	1.3.6.1.4.1.171.12.37.100.0.1
swPortLoopOccurred	The trap is sent when a Port loop occurs. Binding 1. swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.1
swPortLoopRestart	The trap is sent when a Port loop restarts after the interval time. Binding 1. swLoopDetectPortIndex	1.3.6.1.4.1.171.12.41.10.0.2
swVlanLoopOccurred	The trap is sent when a Port with a VID loop occurs. Binding 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.3
swVlanLoopRestart	The trap is sent when a Port with a VID loop restarts after the interval time. Binding 1. swLoopDetectPortIndex 2. swVlanLoopDetectVID	1.3.6.1.4.1.171.12.41.10.0.4
swBpduProtectionUnderAttackingTrap	When the BPDU Protection trap is enabled, if the specific port changes from a normal state to an under attack state, a trap will be sent out. Binding 1. swBpduProtectionPortIndex 2. swBpduProtectionPortMode	1.3.6.1.4.1.171.12.76.4.0.1
swBpduProtectionRecoveryTrap	When the BPDU Protection trap is enabled, if the specific port changes from an under attack state to a normal state, a trap will be sent out. 1. swBpduProtectionPortIndex 2. swBpduProtectionRecoveryMethod	1.3.6.1.4.1.171.12.76.4.0.2
swERPSSFDetectedTrap	When a signal failure occurs, a trap will be generated. Binding 1. swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.1
swERPSSFClearedTrap	When the signal failure clears, a trap will be generated. Binding 1. swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.2
swERPSRPLOwnerConflictTrap	When a conflict occurs, a trap will be generated. Binding 1. swERPSNodeId	1.3.6.1.4.1.171.12.78.4.0.3
dot1agCfmFaultAlarm	A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Binding 1. dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1
swCFMExtAISOccurred	A notification is generated when local MEP enters AIS status. Binding 1. dot1agCfmMdIndex	1.3.6.1.4.1.171.12.86.100.0.1

	2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	
swCFMExtAISCleared	A notification is generated when local MEP exits AIS status. Binding 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.2
swCFMExtLockOccurred	A notification is generated when local MEP enters lock status. Binding 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.3
swCFMExtLockCleared	A notification is generated when local MEP exits lock status. Binding 1. dot1agCfmMdIndex 2. dot1agCfmMaIndex 3. dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.4
swFanFailure	Fan Failure notification. Binding 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.1
swFanRecover	Fan Recover notification. Binding 1. swFanUnitIndex 2. swFanID	1.3.6.1.4.1.171.12.11.2.2.3.0.2
swHighTemperature	High Temperature notification. Binding 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.1
swHighTemperatureRecover	swHighTemperatureRecover Binding 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.2
swLowTemperature	Low Temperature notification. Binding 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.3
swLowTemperatureRecover	Low Temperature notification. Binding 1. swTemperatureUnitIndex 2. swTemperSensorID 3. swTemperatureCurrent	1.3.6.1.4.1.171.12.11.2.2.4.0.4
agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding 1. swMultiImageVersion	1.3.6.1.4.1.171.12.1.7.2.0.7
agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded. Binding 1. unitID 2. agentCfgOperate 3. agentLoginUserName	1.3.6.1.4.1.171.12.1.7.2.0.9
swPowerStatusChg	Power Status change notification. Binding 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.1
swPowerFailure	Power Failure notification. Binding 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	1.3.6.1.4.1.171.12.11.2.2.2.0.2
swPowerRecover	Power Recover notification.	1.3.6.1.4.1.171.12.11.2.2.2.0.3

	Binding 1. swPowerUnitIndex 2. swPowerID 3. swPowerStatus	
swUnitInsert	Unit Hot Insert notification. Binding 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.1
swUnitRemove	Unit Hot Remove notification. Binding 1. swUnitMgmtId 2. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.2
swUnitFailure	Unit Failure notification. Binding 1. swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.3
swUnitTPChange	The stacking topology change notification. Binding 1. swStackTopologyType 2. swUnitMgmtId 3. swUnitMgmtMacAddr	1.3.6.1.4.1.171.12.11.2.2.1.0.4
swUnitRoleChange	The stacking unit role change notification. Binding 1. swStackRoleChangeType 2. swUnitMgmtId	1.3.6.1.4.1.171.12.11.2.2.1.0.5
lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding 1. lldpStatsRemTablesInserts 2. lldpStatsRemTablesDeletes 3. lldpStatsRemTablesDrops 4. lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding 1. lldpRemChassisIdSubtype 2. lldpRemChassisId 3. lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1
dot3OamNonThresholdEvent	A dot3OamNonThresholdEvent notification is sent when a local or remote non-threshold crossing event is detected. A local event is detected by the local entity, while a remote event is detected by the reception of an Ethernet OAM Event Notification OAMPDU that indicates a non-threshold crossing event. Binding 1. dot3OamEventLogTimestamp 2. dot3OamEventLogOui 3. dot3OamEventLogType 4. dot3OamEventLogLocation 5. dot3OamEventLogEventTotal	1.3.6.1.2.1.158.0.2
swSingleIPMSColdStart	The commander switch will send swSingleIPMSColdStart notification to the indicated host when its member generates a cold start notification. Binding 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11
swSingleIPMSWarmStart	The commander switch will send swSingleIPMSWarmStart notification to the indicated host when its member generates a warm start notification. Binding 1.swSingleIPMSID 2.swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.12

swSingleIPMSLinkDown	The commander switch will send swSingleIPMSLinkDown notification to the indicated host when its member generates a link down notification. Binding 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
swSingleIPMSLinkUp	The commander switch will send swSingleIPMSLinkUp notification to the indicated host when its member generates a link up notification. Binding 1.swSingleIPMSID 2.swSingleIPMSMacAddr 3.ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
swSingleIPMSAuthFail	The commander switch will send swSingleIPMSAuthFail notification to the indicated host when its member generates an authentation failure notification. Binding 1. swSingleIPMSID 2. swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
swSingleIPMSnewRoot	The commander switch will send swSingleIPMSnewRoot notification to the indicated host when its member generates a new root notification. Binding 1. swSingleIPMSID 2. swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
swSingleIPMSTopologyChange	The commander switch will send swSingleIPMSTopologyChange notification to the indicated host when its member generates a topology change notification. Binding 1. swSingleIPMSID 2. swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
coldStart	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.3
linkUp	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding 1: ifIndex 2: ifAdminStatus 3: ifOperStatus	1.3.6.1.6.3.1.1.5.4
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this	1.3.6.1.6.3.1.1.5.5

	trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2
risingAlarm	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding 1: alarmIndex 2: alarmVariable 3: alarmSampleType 4: alarmValue 5: alarmFallingThreshold	1.3.6.1.2.1.16.0.2
LLDP	This trap is initialed when a LLDP entry is added to or deleted from remote DB.	1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.0.8802.1.1.2.1.2.2 1.0.8802.1.1.2.1.2.3 1.0.8802.1.1.2.1.2.4 1.0.8802.1.1.2.1.2.5

Appendix E RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: 802.1X (Port-based and Host-based), MAC-based Access Control, Web-based Access Control (WAC), and Japanese Web-based Access Control (JWAC).

The description that follows explains the following RADIUS Attributes Assignment types:

- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign **Ingress/Egress bandwidth by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and the 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0" or more, than the effective bandwidth (100Mbps on an Ethernet port or 1Gbps on a Gigabit port) of the port will be set to no_limited.

To assign **802.1p default priority by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The tables below show the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0-7	Required

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC-based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign **VLAN by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. To use VLAN assignment, RFC3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminatior).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required

Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
 0                   1                   2                   3

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|     Type      |    Length     |      Tag      |   String...

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format	Note
0x01	VLAN name (ASCII)	A tag field of greater than 0x1F is interpreted as the first octet of the following field.
0x02	VLAN ID (ASCII)	
Others (0x00, 0x03 ~ 0x1F, >0x1F)	1. When the switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the switch will check all existed VLAN ID and check if there is one matched. 2. If the switch can find one matched, it will move to that VLAN. 3. If the switch can not find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”. 4. Then it will check that it can find out a matched VLAN Name.	

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC-based Access Control authentication is successful, the port will be added to VLAN 3. However, if the user does not configure the VLAN attribute and authenticates successfully, the port will be kept in its original VLAN. If the VLAN attribute configured on the RADIUS server does not exist, the port will not be assigned to the requested VLAN.

To assign **ACL by RADIUS Server**, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for an ACL. The RADIUS ACL assignment is only used in MAC-based Access Control.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	12 (for ACL profile) 13 (for ACL rule)	Required

Attribute-Specific Field	Used to assign the ACL profile or rule.	ACL Command For example: ACL profile: **create access_profile profile_id 6 profile_name 1 ethernet vlan 0xFFF;** ACL rule: **config access_profile profile_id 6 add access_id auto_assign ethernet vlan_id 1 port all deny;**	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL profile: **create access_profile profile_id 6 profile_name 1 ethernet**; ACL rule: **config access_profile profile_id 6 add access_id auto_assign ethernet**), and the 802.1X or MAC-based Access Control or WAC authentication is successful, the device will assign the ACL profiles and rules according to the RADIUS server. For more information about the ACL module, please refer to Chapter 22 Access Control List (ACL) Commands.